HIRSCHMANN

A BELDEN BRAND

User Manual

Operation and Maintenance Guide
OpenBAT Family

Technical Support
https://hirschmann-support.belden.eu.com

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Rel. 8.80 - 09/2013 – 13.9.13

Contents

Safety instructions

Important Information

Notice: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

⚡ The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

⚠ This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

Related Documents

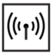
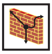
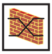
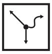
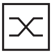
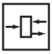
Title of the document
OpenBAT Configuration and Administration Guide
OpenBAT Installation User Manual
Reference Manual Command Line Interface OpenBAT Family
WLAN Outdoor Guide
Antenna Guide Wireless LAN Antennas of the OpenBAT family

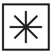
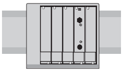
Key

The designations used in this manual have the following meanings:

▶	List
□	Work step
	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface
🟦	Execution in the Graphical User Interface (Web-based Interface user interface)
🟩	Execution in the Command Line Interface user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

1 Project Management with LANconfig

1.1 Starting LANconfig

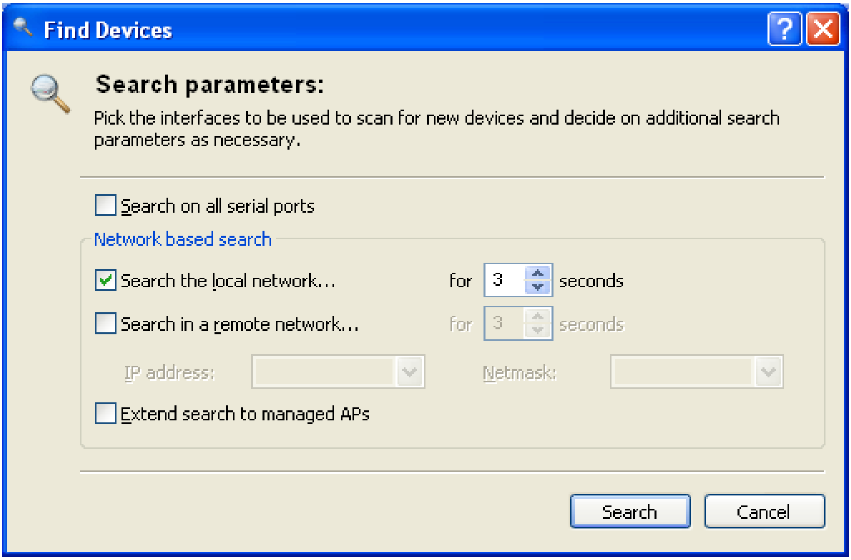
When you first start-up LANconfig, it automatically searches for devices on the local network. If it discovers an unconfigured device on the local area network (LAN), LANconfig automatically launches the setup wizard for that device.

Note: If a firewall is activated on your PC, LANconfig might not be able to find a new device in the LAN. In this case, deactivate the firewall during device discovery and configuration.

1.1.1 Finding New Devices

You can manually instruct LANconfig to initiate a search for new LAN devices. To begin a search:

☐ Select `File:Find Devices`. The ‘Find Devices’ dialog opens:



Find Devices

Search parameters:

Pick the interfaces to be used to scan for new devices and decide on additional search parameters as necessary.

☐ Search on all serial ports

Network based search

☑ Search the local network... for 3 seconds

☐ Search in a remote network... for 3 seconds

IP address: Netmask:

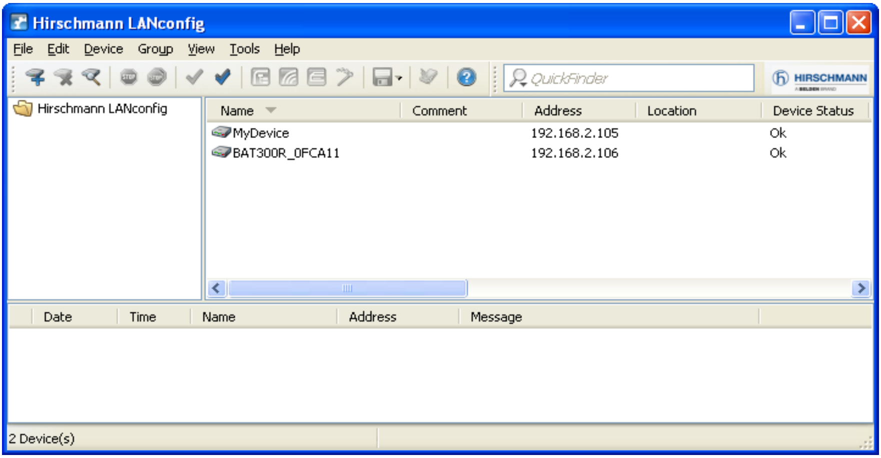
☐ Extend search to managed APs

☐ Use the ‘Find Devices’ dialog to specify the scope of the search, including:

- the networks to be searched: local, remote, or both
- how long each network search should last
- whether the search should include all serial ports.

Selecting the ‘Search the local network’ option is usually sufficient. Click ‘OK’ and the search begins.

After LANconfig finishes the search, it displays a list of all the devices it has found, including each device name, IP address, and device status:



Name	Comment	Address	Location	Device Status
MyDevice		192.168.2.105		Ok
BAT300R_0FCA11		192.168.2.106		Ok

1.1.2 Using the Integrated Help Function

To assist you in using LANconfig, an integrated help feature is provided. Click on the 'Help' question mark button located at the top right in any dialog and then on a parameter's name to call up context-sensitive help.

1.2 LANconfig Behavior at Windows Startup

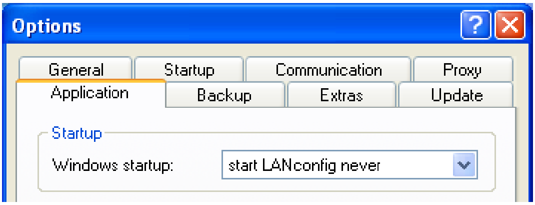
LANconfig can be configured to run automatically when the Windows operating system starts up. Options include:

- Start LANconfig never: LANconfig does not start during the Windows startup. If required, start LANconfig manually. This is the default setting.
- Start LANconfig always: LANconfig starts automatically after a successful Windows startup.
- Start LANconfig like before: LANconfig startup behavior depends on its run state before the last Windows shutdown. If LANconfig had been running, it will start automatically after the Windows startup; otherwise, LANconfig will not start automatically.

Note: When you change from ‘never’ to either of the other selections, LANconfig writes or deletes an entry in the autostart section of the system registry. Firewalls on the configuration computer or the operating system itself may interpret these changes as an attack and may alert you or even block the access. Because you make these changes in the Windows startup intentionally, you can ignore these alerts and confirm the new startup behavior.

To configure LANconfig behavior at Windows startup:

□ Select `Tools : Options` to open the ‘Options’ dialog, then select the ‘Application’ tab:



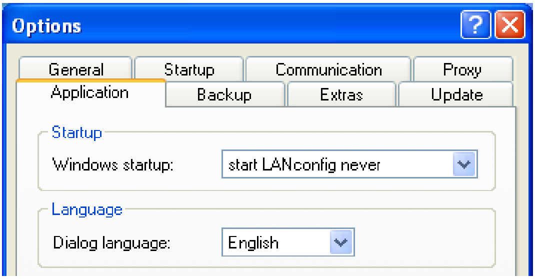
Windows startup: start LANconfig never

□ Select a ‘Windows startup’ option, as described above.

1.3 Setting the GUI Language

The graphical user interface (GUI) language for LANconfig, LANmonitor or WLANmonitor can be set to either German or English. To change the GUI for LANconfig:

☐ Select `Tools : Options` to open the ‘Options’ dialog, then select the ‘Application’ tab:



Startup

Windows startup: start LANconfig never

Language

Dialog language: English

☐ Select a ‘Dialog language’ option: German or English.

Note: In both LANmonitor and WLANmonitor, the language setting can be found in the `Tools : Options : General` dialog.

1.4 Flexible group configuration with LANconfig

Note: Flexible group configuration is available with all its features from HiLCOS version 8.60 on.

When managing many devices, it is helpful to manage a selection of configuration parameters together for a group of devices. This is useful, for example, for identical SSID settings in WLAN access points. It does not make sense to copy a complete configuration file from another device, as the device also takes over device-specific parameters such as the IP address in the process. With the group configuration in LANconfig you can conveniently set group configuration parameters and thus manage multiple devices at the same time.

By assigning multiple devices to a group configuration, you combine these devices into a collectively managed group. The group configuration files with shared parameters for a group of Hirschmann devices are stored like complete configuration files on the hard disk or on a server. For the configuration of entire device groups, LANconfig creates references to these group configuration files. These references are convenient links between the device entries in LANconfig and the group configuration files.

LANconfig provides “group templates”, which are templates for creating group configurations. You have the option to adjust the scope of the group contingent individually, to include additional configuration parameters as group parameters, or to remove proposed group parameters. You can save these created configurations as your own templates for creating new groups.

Note: Later you only have the option to change your created group configuration templates, but the LANconfig basic templates are not affected by this.

From HiLCOS version 8.60 on, the following group configurations are available as basic templates:

- **Hirschmann Group Template WLAN:** Contains all the parameters that are usually managed together on WLAN devices.
- **Hirschmann Group Template WLC:** Contains as many parameters of Hirschmann WLC devices as possible, to minimize the need for individual configuration when operating a cluster of WLCs.
- **Hirschmann Group Template empty:** Does not contains a pre-selection of group parameters, and is used as a basis for creating your own group templates which the device cannot meaningfully derive from any WLAN or WLC template.

1.4.1 Creating a group configuration

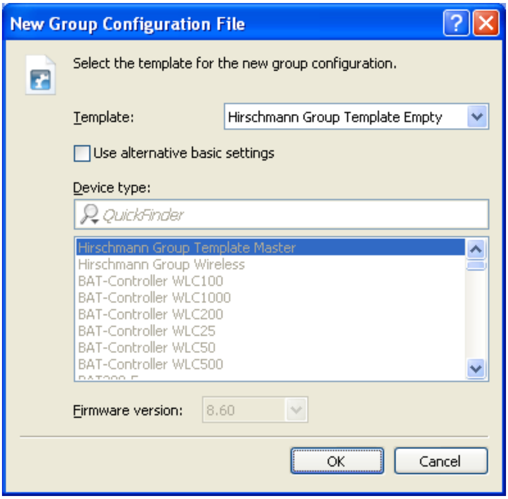
A prerequisite for using the group configuration is that the devices are grouped into folders. These LANconfig folders contain the group entries for which a shared configuration of the group configuration parameters makes sense, as well as a reference to the group configuration.

Note: With a group configuration you manage the device parameters that are shared by all the assigned devices. A device-specific configuration relates to the parameters that are device-specific.

New group configuration file

☐ Create a new folder that contains the devices to be grouped. There are 2 ways for you to create this folder:

- ☐ Right-click an existing folder in the folder view and select “New folder with group configuration”. Now the configuration dialog creates a new order below the clicked directory level and starts the template selection for creating a new group configuration.
- ☐ In the order view, right-click the directory in which you want to create the new folder. In the context dialog, select “New folder” and enter a name. Use the mouse to move the devices to be grouped into this new folder. Now right-click the new folder, and in the context menu select the entry “New Group Configuration”.



New Group Configuration File

Select the template for the new group configuration.

Template: Hirschmann Group Template Empty

□ Use alternative basic settings

Device type:

QuickFinder

Hirschmann Group Template Master
Hirschmann Group Wireless
BAT-Controller WLC100
BAT-Controller WLC1000
BAT-Controller WLC200
BAT-Controller WLC25
BAT-Controller WLC50
BAT-Controller WLC500

Firmware version: 8.60

Figure 1: Creating a new group configuration from a template file

□ Select a template and click “OK”. Alternatively, you can select the basic configuration settings of a particular device in dependence on the used firmware version as an initial for the group configuration.

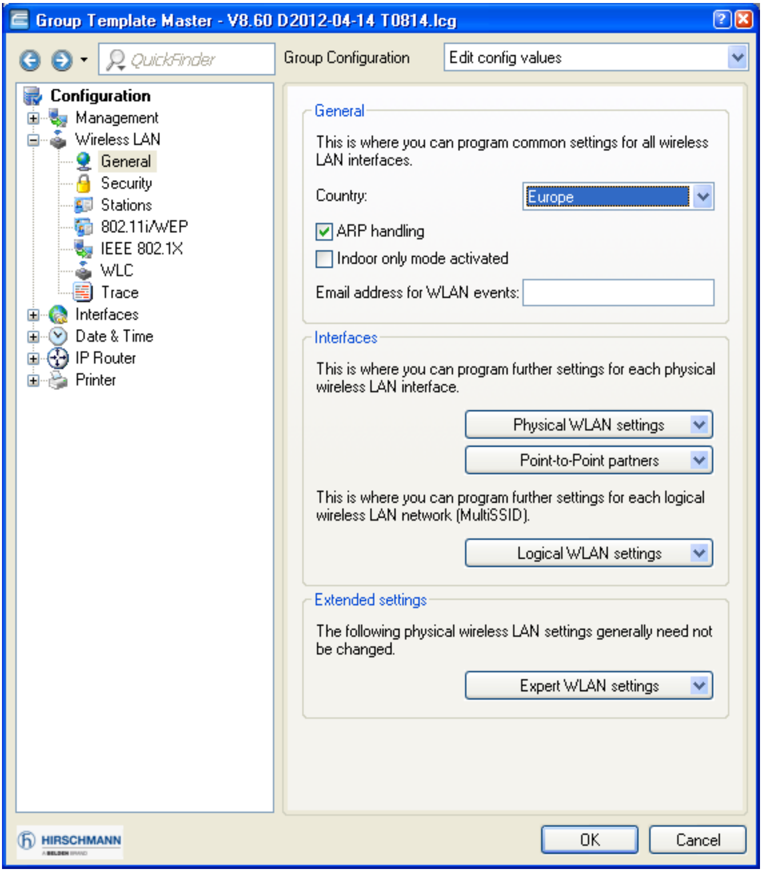
Note: If you have previously saved your own group templates, these also appear in the selection list of templates.

□ A configuration dialog opens. Here you can choose from 2 alternative processing modes, which you select via the “Group Configuration” list:

  □ “Edit config values” mode.

  □ “Select group parameter” mode.

□ The configuration dialog starts with the “Edit config values” view. In this view you only see the parameters of the group that are managed together. You have the option to set these to the desired values and content. All parameters that apply to the individual devices are hidden.



Group Configuration: Edit config values

General

This is where you can program common settings for all wireless LAN interfaces.

Country: Europe

☑ ARP handling

☐ Indoor only mode activated

Email address for WLAN events:

Interfaces

This is where you can program further settings for each physical wireless LAN interface.

Physical WLAN settings

Point-to-Point partners

This is where you can program further settings for each logical wireless LAN network (MultiSSID).

Logical WLAN settings

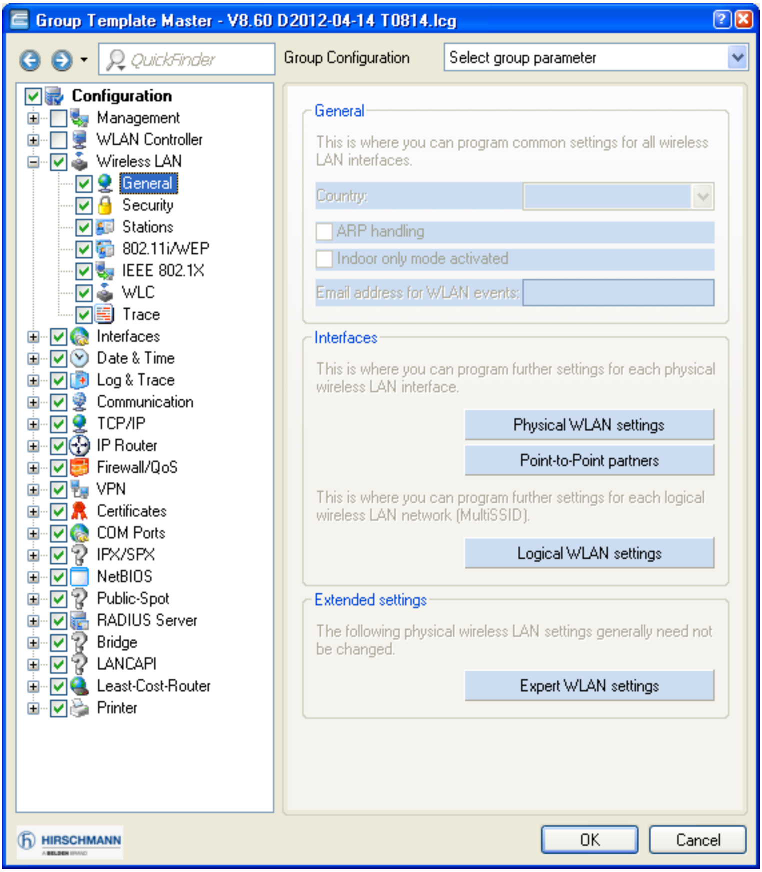
Extended settings

The following physical wireless LAN settings generally need not be changed.

Expert WLAN settings

Figure 2: View of the shared properties of a device group

☐ In the “Select group parameter” configuration mode, you select/deselect from all the available parameters those which you require for an adjusted group configuration.



This is where you can program common settings for all wireless LAN interfaces.

This is where you can program further settings for each physical wireless LAN interface.

This is where you can program further settings for each logical wireless LAN network (MultiSSID).

The following physical wireless LAN settings generally need not be changed.

Figure 3: Selecting the group parameters for viewing

Elements displayed in light-blue are selected for use in the group configuration. Left-click an element to change its selection status.

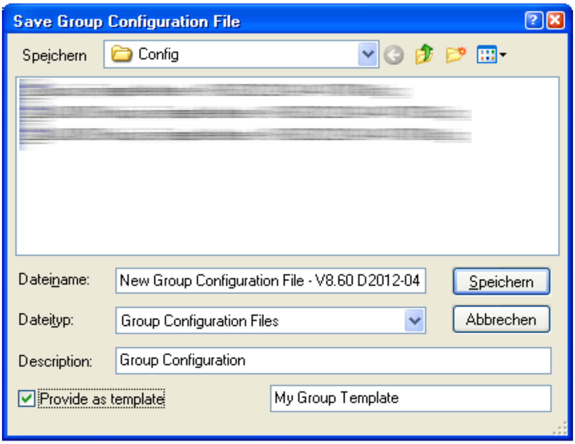
Note the following special features:

- For tables with statically preset lines (e.g. interface-related tables such as logical WLAN settings), you have the option to copy individual parameters into the group configuration. You can access some of these parameters in LANconfig via the pull-down menus for buttons.
- For tables with dynamically created lines (e.g. the routing table), you can only select/deselect the entire table for the group configuration.
- You have the option only to completely select/deselect the firewall for the group configuration.

□ To finish, click “OK”.

□ Specify where the device saves the created group configuration. The default setting is the directory you entered under `Extras:Options:Backup:Backup Path` (default: "\config\")

□ In the future, LANconfig offers you this group configuration as your own template for creating other group configurations when you activate the option “Provide as template”. Assign a meaningful name to this.



Speichern: Config

Dateiname: New Group Configuration File - V8.60 D2012-04

Dateityp: Group Configuration Files

Description: Group Configuration

☑ Provide as template: My Group Template

Figure 4: Saving a group configuration as a template

Note: Later you also have the option to create a template from an existing group configuration. To do this, right-click the corresponding group configuration in the corresponding LANconfig folder, activate “Provide as template” in the context menu, and enter a meaningful name.

☐ Click “Save” to complete the operation.

Note: The group configuration saves all the parameters in a group configuration file. In the process, the device also saves the parameters with the standard values that are not changed. Use the scripting functions to only read the parameters that differ from the standard settings from the device and copy them to other devices, if applicable.

The assigned group configuration file appears in the list of entries with the description “Group Configuration”. You change the name of the group configuration via the properties. To do this, right-click the entry and in the context menu select the entry “Properties”.

Note: In LANconfig you have the option to create multiple references to the same group configuration. Where there is multiple assignment of the same group configuration in different LANconfig folders, when the group parameters are changed this affects the devices in all the relevant folders.

Using an existing group configuration file

In some cases it makes sense to structure the devices managed with LANconfig differently in folders than would be required by the group configuration. For example, you assign the devices in location-specific folders to the same groups. To avoid redundant group configuration files for every folder, create references to a shared file in multiple folders.
To use an existing group configuration file for a group of devices, right-click the desired folder, and in the context menu select the entry “Add group configuration”.

In the following dialog select the existing group configuration file and thus create a reference to this file in the folder.

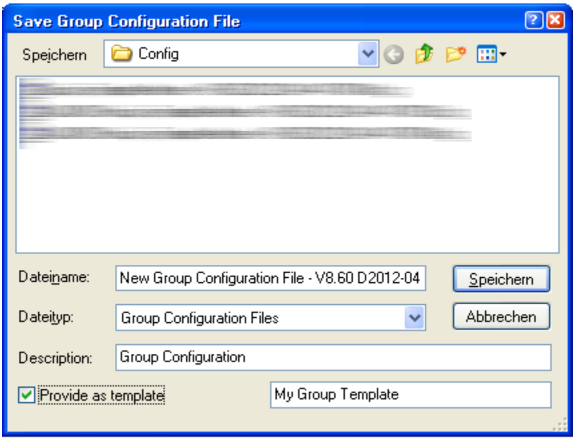
Note: If you create additional devices in a group folder, or change an existing group configuration, LANconfig informs you that there is an update for the corresponding devices. You perform this update directly afterwards, or later via the context menu. Note that changing the group configuration file also results in changes to the respective group configurations in various folders.

1.4.2 Enhancements in the menu system

`Group`

Under the “Group” menu item you manage group configurations.

- `New Group Configuration`
  Under `Group:New Group Configuration` you create a new group configuration in the current folder.
- `New Folder with Group Configuration`
  Under `Group:New Folder with Group Configuration` you create a new subfolder with a new group configuration in the current folder.
- `Add Group Configuration`
  Under `Group:Add Group Configuration` you save an existing group configuration in the active folder. For this, you select the corresponding file.



Dateiname: New Group Configuration File - V8.60 D2012-04

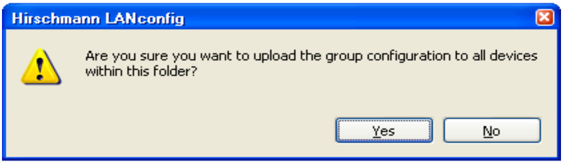
Dateityp: Group Configuration Files

Description: Group Configuration

☑ Provide as template: My Group Template

Figure 5: Selecting a group configuration

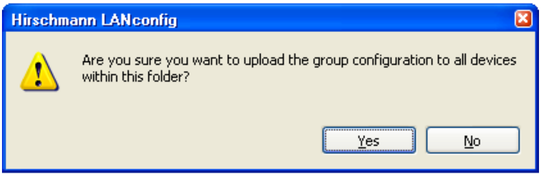
- `Edit Group Configuration`
  Under `Group:Edit Group Configuration`, you can edit the selected group configuration.
  Set the parameters in the configuration as they are to apply for the whole group. When closing the configuration dialog, LANconfig asks you to save the corresponding group configuration file at a location of your choice.
- `Update All Devices`
  Under `Group:Update All Devices` you can use the selected and activated group to update all the devices in the current folder.


Hirschmann LANconfig

Are you sure you want to upload the group configuration to all devices within this folder?

Figure 6: Uploading the group configuration to all devices in a folder

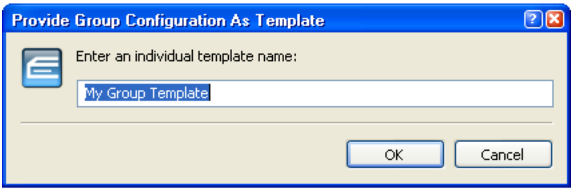
- ▶ `Update Recommended Devices`
  Under `Group:Update Recommended Devices` you can use the selected and activated group to update the recommended devices in the current folder.


Hirschmann LANconfig

Are you sure you want to upload the group configuration to all devices within this folder?

Figure 7: Uploading the group configuration to all devices in a folder

- ▶ `Provide as Template`
  Under `Group:Provide as Template` you can define the selected group configuration as a template for future group configurations.


Provide Group Configuration As Template

Enter an individual template name:

My Group Template

Figure 8: Saving a group configuration as a template

- `Active`
  Under `Group:Active` you activate or deactivate the selected group configuration.

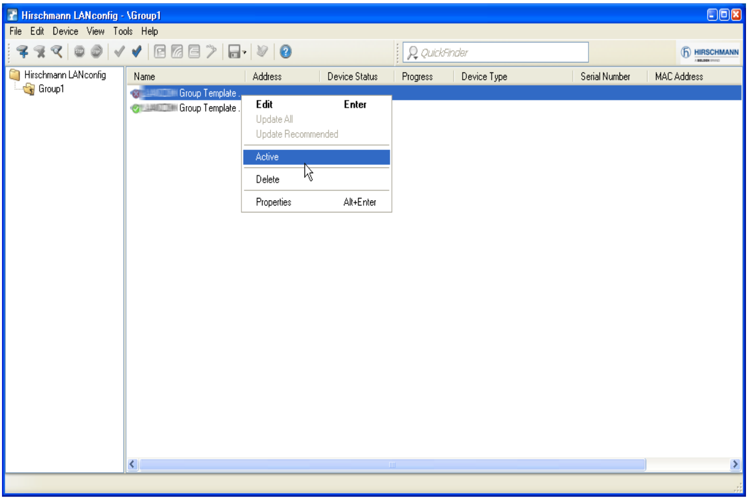
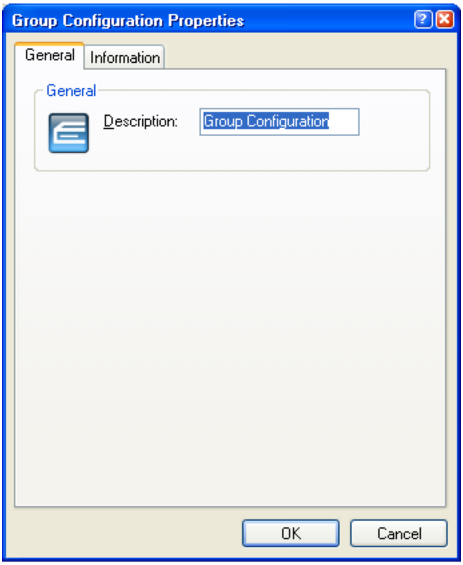


Figure 9: Activating the selected group configuration

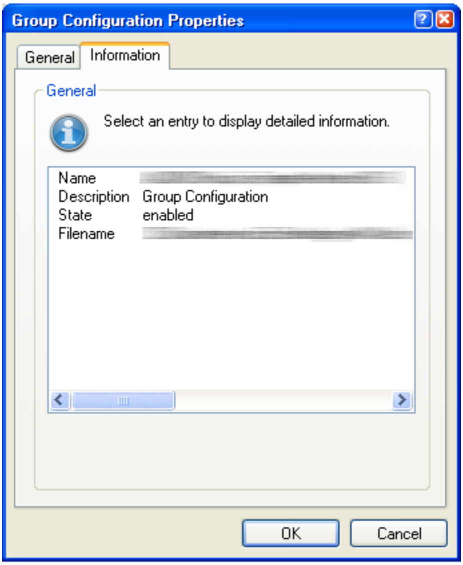
- `Delete`
  With `Group:Delete` you delete the selected group configuration.
- `Properties`
  Under `Group:Properties` you display information for an existing group configuration. For this, you select the corresponding file.
  The `General` tab displays the description of the group configuration.



Description: Group Configuration

Figure 10: General properties of a group configuration

The `Info` tab displays the name, status and file name of the group configuration.



Select an entry to display detailed information.

Name	[redacted]
Description	Group Configuration
State	enabled
Filename	[redacted]

Figure 11: “Info” tab page

1.5 User-Specific Settings for LANconfig

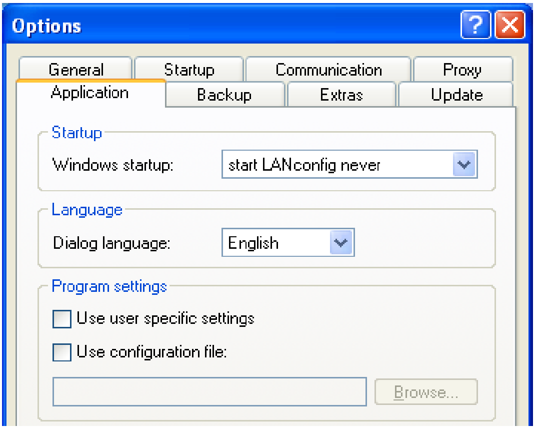
When LANconfig shuts down, program settings are saved to the file “lanconf.ini” located in the program directory. This includes the displayed devices, directory structure, selected language, etc. When LANconfig starts-up, it reads this ini file and restores the previous status of the software.

As an alternative to the .ini file in the program directory, the program settings can be read from another source. Your user directory can be chosen, or any other lanconf.ini file from any location:

- By selecting the user directory, users can save their personal settings even if they exclusively have read authorization for the program directory.
- Selecting an alternative storage location can be used, for example, to transfer program settings to any other LANconfig installation, or to save the program settings to a central location in the network for use by multiple users.

To configure user-specific LANconfig settings:

☐ Select `Tools : Options`, the click the ‘Applications’ tab to open that dialog.



Windows startup: start LANconfig never

Dialog language: English

☐ Use user specific settings

☐ Use configuration file:

The following parameters can be set in this dialog:

- Use user-specific settings:
  Activates the use of the lanconf.ini file in the current user’s directory: ...\User\Application Files\OpenBAT\LANconfig. When you activate this option, changes to the program settings are saved to this ini file. When you activate this option in parallel with the “Use configuration file” option, LANconfig uses the file selected here when it starts, and it stores the changes in this file. In the default setting, this option is deactivated.
- Use configuration file:
  This activates the usage of the lanconf.ini from the given directory. With this option activated, changes to the program settings are saved to the selected ini file. De-selected by default.

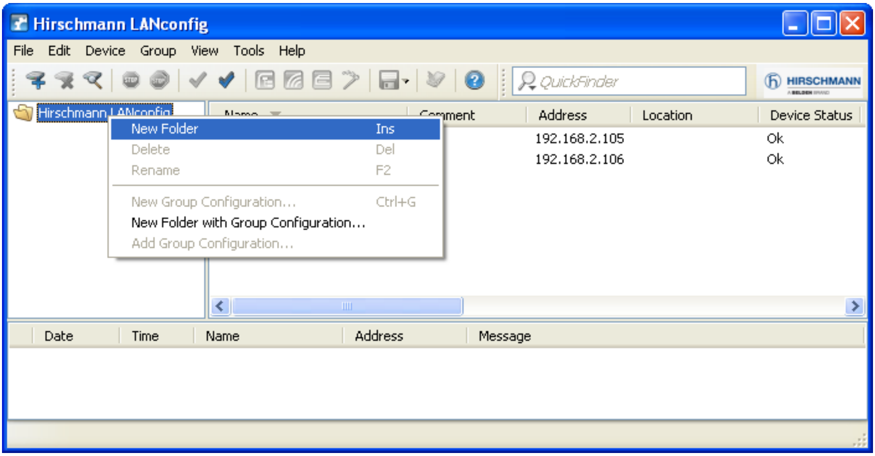
  Note: The file you select needs to be a valid LANconfig settings file.

If neither of the two options is activated, the ini file from the program directory will be used.

1.6 Directory Structure

LANconfig uses a directory structure to provide an overview when managing multiple devices. The arrangement of devices in folders effects the display of the devices within LANconfig. The organization of the folders has no influence on the actual configuration of the devices. Folders dedicated to projects or customers can be set up to organize the relevant devices:

- Create a new folder by right-clicking on the parent directory and selecting “New Folder” from the context menu.


Hirschmann LANconfig
File Edit Device Group View Tools Help
QuickFinder
HIRSCHMANN
Hirschmann LANconfig
New Folder Ins
Delete Del
Rename F2
New Group Configuration... Ctrl+G
New Folder with Group Configuration...
Add Group Configuration...

Name	Comment	Address	Location	Device Status
		192.168.2.105		Ok
		192.168.2.106		Ok

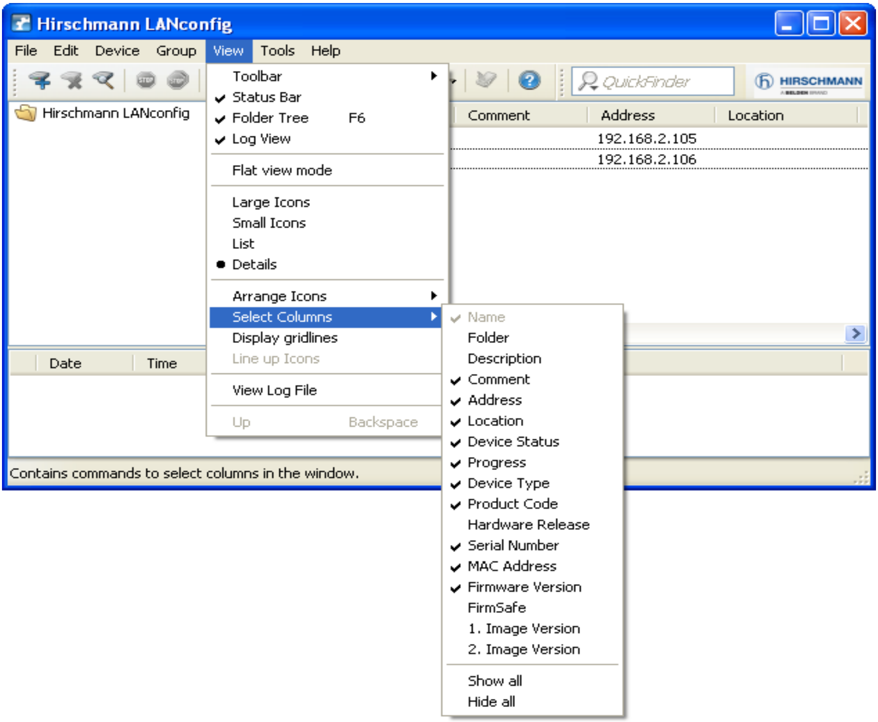
Date	Time	Name	Address	Message

- Use the mouse to drag and drop the devices into the appropriate folder. Devices can also be moved from one folder to another using this method.

The directory structure in the left side of the LANconfig window can be switched on and off using either the `F6` function key or the command `View : Folder Tree.`

1.7 Increasing the Number of Columns in LANconfig

You can attain a better overview and quicker orientation of your project in LANconfig by adding to or subtracting from the columns that describe the project’s devices. To edit the specific parameters included as column headers for all devices, select `View : Select Columns`, then choose the parameters to be displayed as columns.



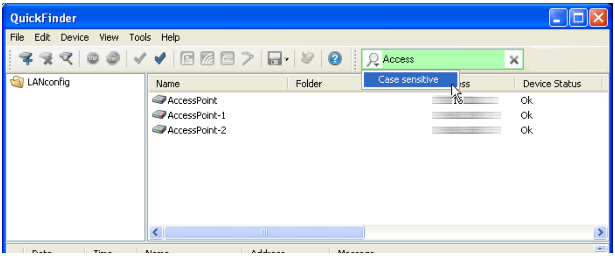
Contains commands to select columns in the window.

Use the menu item ‘Select Columns’ command to display the device properties you wish to view. The following properties can be displayed:

- Name
- Folders
- Description
- Comment
- Address
- Location
- Device Status
- Progress
- Device type
- Product code
- Hardware release
- Serial number
- MAC address
- Firmware version
- FirmSafe
- 1. Image version
- 2. Image version

1.8 Searching with QuickFinder

The configuration dialogs in LANconfig, LANmonitor and WLANmonitor are comprised of numerous areas, parameters and their values, and tables. The QuickFinder helps you search for the desired value. In the main view of LANconfig, you will find QuickFinder in the tool bar. Enter a search term in the search window to reduce the number of devices displayed. LANconfig searches through all the values available in the columns of the device list – including the columns currently hidden. Click the symbol beside the magnifying glass to make the search case-sensitive.



Name	Folder	...ss	Device Status
AccessPoint			Ok
AccessPoint-1			Ok
AccessPoint-2			Ok

Figure 12: QuickFinder in the main view of LANconfig

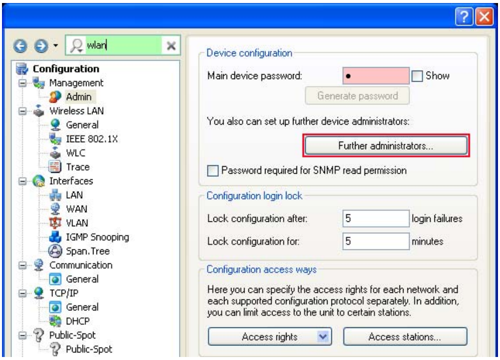
When you search for a specific value or term in LANconfig or the configuration, the QuickFinder quickly shows you in the configuration dialogs of LANconfig all the places that contain the character string you are searching for.

□ Start LANconfig.

□ Open the configuration of the device you want to search in.

□ Enter the desired term in the search field, e.g. ‘wlan’. The search is not case-sensitive. You can enter parts or words or numbers, as well as complete search terms. Spaces in the search terms search for character strings that contain corresponding spaces. However, the search function does not support wildcards.

The configuration tree in the left area of LANconfig is now reduced to all the areas that contain the search term:



Device configuration

Main device password: ● □ Show

You also can set up further device administrators:

□ Password required for SNMP read permission

Configuration login lock

Lock configuration after: 5 login failures

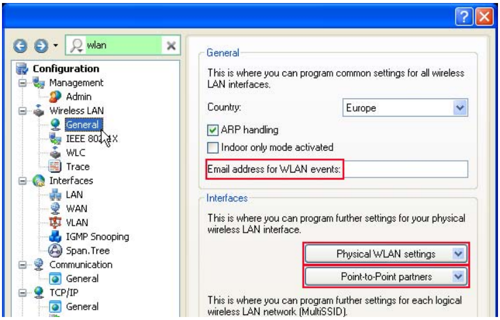
Lock configuration for: 5 minutes

Configuration access ways

Here you can specify the access rights for each network and each supported configuration protocol separately. In addition, you can limit access to the unit to certain stations.

Figure 13: Searching in the configuration dialog of LANconfig using the QuickFinder

Select one of the areas in the configuration tree (e.g. ‘WLAN/General’) to display the corresponding search results framed in color in the configuration dialog:



General

This is where you can program common settings for all wireless LAN interfaces.

Country: Europe

☑ ARP handling

□ Indoor only mode activated

Email address for WLAN events:

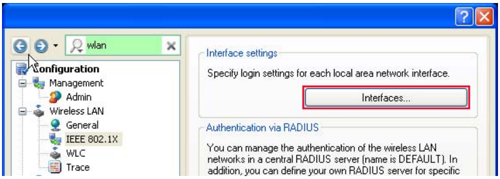
Interfaces

This is where you can program further settings for your physical wireless LAN interface.

This is where you can program further settings for each logical wireless LAN network (MultiSSID).

Figure 14: Selection of search results in QuickFinder

Use the ‘Forward’ and ‘Back’ navigating buttons to the left of the search field to scroll to the dialogs you visited last:

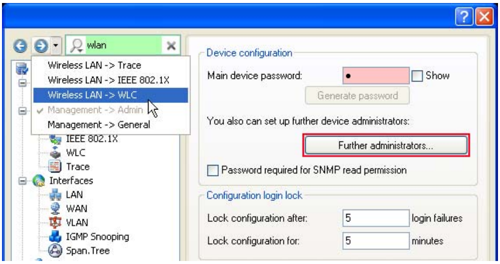


Specify login settings for each local area network interface.

You can manage the authentication of the wireless LAN networks in a central RADIUS server (name is DEFAULT). In addition, you can define your own RADIUS server for specific

Figure 15: Navigating in the search results of the QuickFinder

To get faster access to the last 10 dialogs you visited, click on the arrow to the right of the ‘Forward’ button:



Main device password: ● □ Show

You also can set up further device administrators:

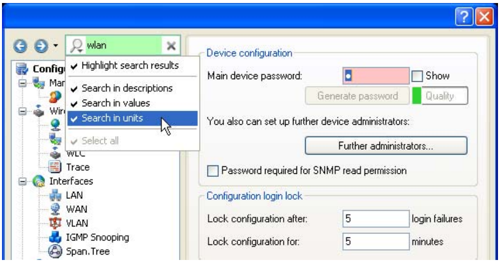
□ Password required for SNMP read permission

Lock configuration after: 5 login failures

Lock configuration for: 5 minutes

Figure 16: Fast access to the search results of the QuickFinder

Click the X to the right of the search field to delete the search and display all the entries in the configuration tree again. To optionally reduce the search results, select areas that you want LANconfig to include in the search. To do this, click the magnifying glass to the left of the search field and activate or deactivate the desired areas. Here you also specify whether the search highlights the hits in color or only reduces the configuration tree to the dialogs found:



wlan

✓ Highlight search results

✓ Search in descriptions

✓ Search in values

✓ Search in units

✓ Select all

Device configuration

Main device password: ● □ Show

You also can set up further device administrators:

□ Password required for SNMP read permission

Configuration login lock

Lock configuration after: 5 login failures

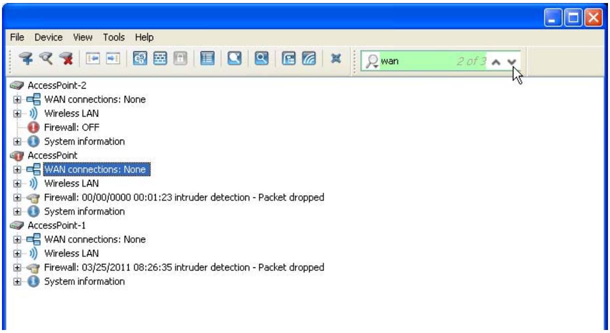
Lock configuration for: 5 minutes

Figure 17: Selecting the search areas for QuickFinder

Note: When the configuration is closed, LANconfig deletes the setting for the search areas and the list of the last dialogs visited.

1.8.1 QuickFinder in the LANmonitor

Depending on the application, the LANmonitor shows multiple devices that could contain the search term. After the search is started, LANmonitor initially highlights the first find. Go to the next find using either the arrow buttons at the right side of the search window or with the key combination Ctrl+F3, or use the key combination Ctrl+Shift+F3 to go back to the previous find.

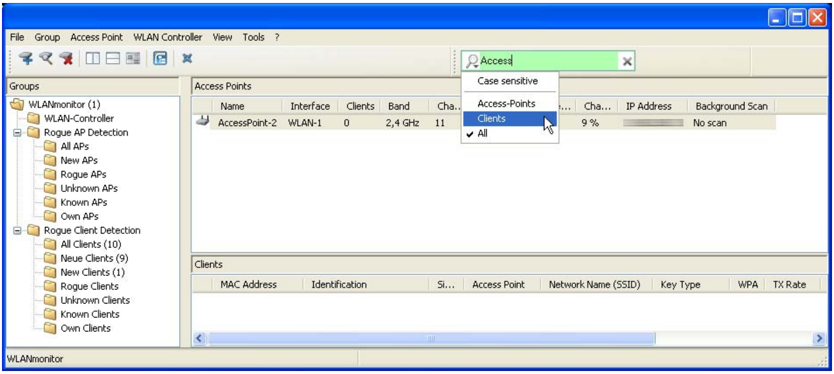


AccessPoint-2
WAN connections: None
Wireless LAN
Firewall: OFF
System information
AccessPoint
WAN connections: None
Wireless LAN
Firewall: 00/00/0000 00:01:23 intruder detection - Packet dropped
System information
AccessPoint-1
WAN connections: None
Wireless LAN
Firewall: 03/25/2011 08:26:35 intruder detection - Packet dropped
System information

Figure 18: QuickFinder in the LANmonitor

1.8.2 QuickFinder in the WLANmonitor

The WLANmonitor includes both access points and WLAN clients. When you click on the magnifying glass on the left side of the search window, you open a context menu for selecting the scope of the search. Depending on the application, you select only the access points, only the clients, or all entries.



Access

Access Points

Name	Interface	Clients	Band	Cha..	...	Cha...	IP Address	Background Scan
AccessPoint-2	WLAN-1	0	2,4 GHz	11		9 %		No scan

Clients

MAC Address	Identification	Si...	Access Point	Network Name (SSID)	Key Type	WPA	TX Rate

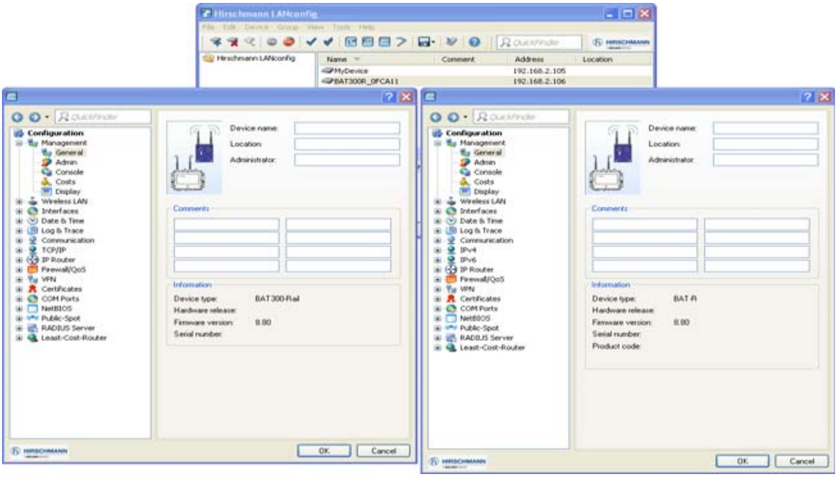
Figure 19: QuickFinder in the WLANmonitor

For example, if you have entered specific settings for your Internet provider in the configuration, by simply entering the name you can find all the positions in the configuration that relate to this provider. Specifically, the search includes the following areas:

- Entries in the configuration tree
- Designations for the areas (sections) in the individual configuration dialogs.
- Parameters
- Values of the parameters
- Explanatory texts in the dialogs
- Names of the tables
- Names of the table columns

1.9 Multithreading

The management of larger projects can be aided by simultaneously opening up configuration windows for multiple devices to compare similarities and differences. LANconfig allows multiple configuration dialogs to be opened at the same time ("multithreading"). After opening the configuration for a device, simply open up additional configurations from the device list in LANconfig. All of the configurations can be processed in parallel.



Hirschmann LANconfig

Name	Comment	Address	Location
MyDevice		192.168.2.105	
BAT300R_0FCA11		192.168.2.106	

Information

Device type: BAT300-Rail
Hardware release:
Firmware version: 8.80
Serial number:

Information

Device type: BAT-R
Hardware release:
Firmware version: 8.80
Serial number:
Product code:

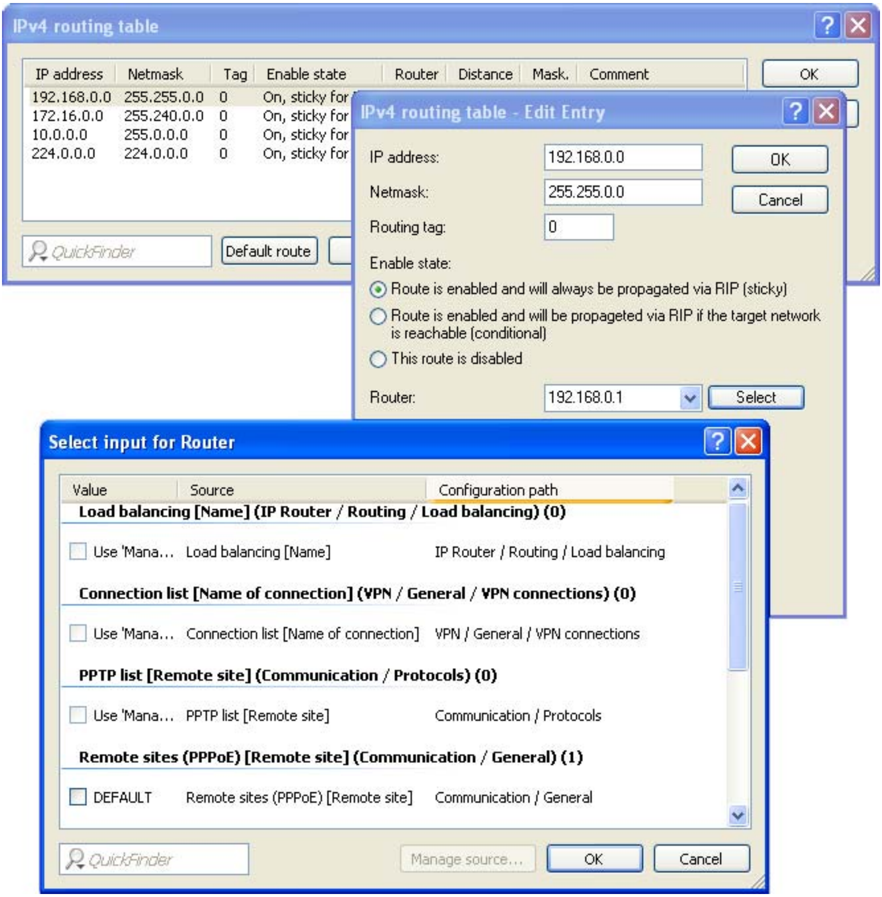
Note: Cut and paste can be used to transfer content between the configuration windows via the Windows clipboard.

Multithreading allows changes to both the internal configurations of the available devices and to the configuration files. Each configuration is written separately to the file and to the device when the dialog is closed.

1.10 Quick Links for Managing Source Tables

Values can be selected from an input field after they have previously been specified in one or more tables. So-called Quicklinks offer you a direct way to manage these source tables. This allows you to bypass the default configuration order. Instead of creating new elements after first exiting the current selection, you can create these items directly if necessary. These new elements are immediately available for selection.

To clarify the structure of the configuration, LANconfig shows the configuration path apart along with the individual sources. If the configuration parameters can be chosen from multiple source tables, LANconfig groups the entries accordingly. For each group, LANconfig additionally specifies the number of entries contained.



IPv4 routing table

IP address	Netmask	Tag	Enable state	Router	Distance	Mask.	Comment
192.168.0.0	255.255.0.0	0	On, sticky for				
172.16.0.0	255.240.0.0	0	On, sticky for				
10.0.0.0	255.0.0.0	0	On, sticky for				
224.0.0.0	224.0.0.0	0	On, sticky for				

IPv4 routing table - Edit Entry

IP address: 192.168.0.0

Netmask: 255.255.0.0

Routing tag: 0

Enable state:

- ● Route is enabled and will always be propagated via RIP (sticky)
- ○ Route is enabled and will be propageted via RIP if the target network is reachable (conditional)
- ○ This route is disabled

Router: 192.168.0.1

Select input for Router

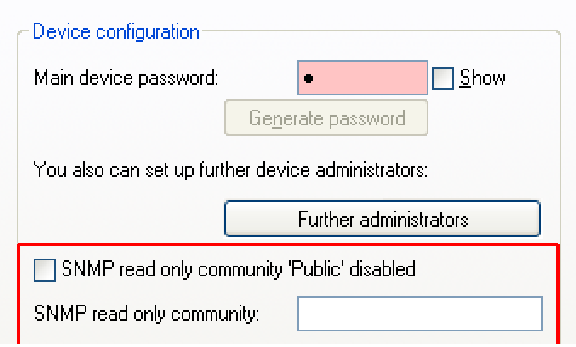
Value	Source	Configuration path
Load balancing [Name] (IP Router / Routing / Load balancing) (0)		
□ Use 'Mana...	Load balancing [Name]	IP Router / Routing / Load balancing
Connection list [Name of connection] (VPN / General / VPN connections) (0)		
□ Use 'Mana...	Connection list [Name of connection]	VPN / General / VPN connections
PPTP list [Remote site] (Communication / Protocols) (0)		
□ Use 'Mana...	PPTP list [Remote site]	Communication / Protocols
Remote sites (PPPoE) [Remote site] (Communication / General) (1)		
□ DEFAULT	Remote sites (PPPoE) [Remote site]	Communication / General

1.11 Password Protection for SNMP Read-Only Access

You can use a password to protect the read-only access to a OpenBAT device via SNMP - e.g. with LANmonitor. This function uses the same user data that you use for the configuration access to the OpenBAT device with LANconfig. When you have activated this function, enter the required user data before you access the device via SNMP.

1.11.1 Requiring a Password for SNMP Read-only Access

You can activate the password requirement for SNMP read-only access in the device configuration in LANconfig for that device. In the `Configuration : Management : Admin` dialogue select the setting "SNMP read only community 'Public' disabled".



Device configuration

Main device password: ● □ Show

You also can set up further device administrators:

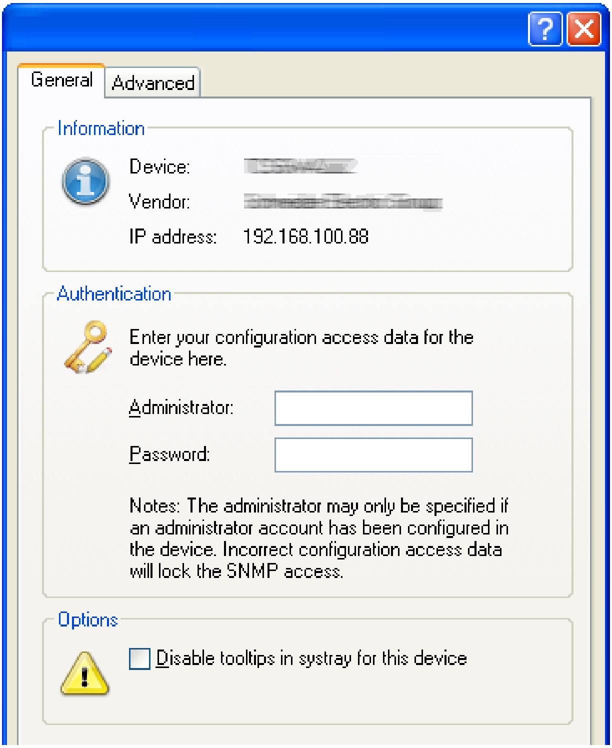
□ SNMP read only community 'Public' disabled

SNMP read only community:

1.11.2 Configuring User Information for SNMP Access

Create the user data in LANmonitor separately for each device. Carry out the following steps:

- □ In LANmonitor, generate a list of found devices using the `File : Find Devices` command.
- □ Highlight a device, click the right mouse button, and select ‘Options...’ from the pop-up menu.
- □ In the ‘Options’ dialog, click the ‘General’ tab to display that dialog:



General | Advanced

Information

Device: [redacted]

Vendor: [redacted]

IP address: 192.168.100.88

Authentication

Enter your configuration access data for the device here.

Administrator:

Password:

Notes: The administrator may only be specified if an administrator account has been configured in the device. Incorrect configuration access data will lock the SNMP access.

Options

□ Disable tooltips in systray for this device

- □ Enter values for the ‘Administrator’ and ‘Password’ parameters.

The access rights available to the defined administrator depend upon the rights granted to that administrator in LANconfig or WEBconfig for the specific device. You can create an administrator profile, including password and function rights at the following location:

```
Configuration : Management : Admin :
Further administrators...
```

1.12 Device-Specific Settings for Communication Protocols

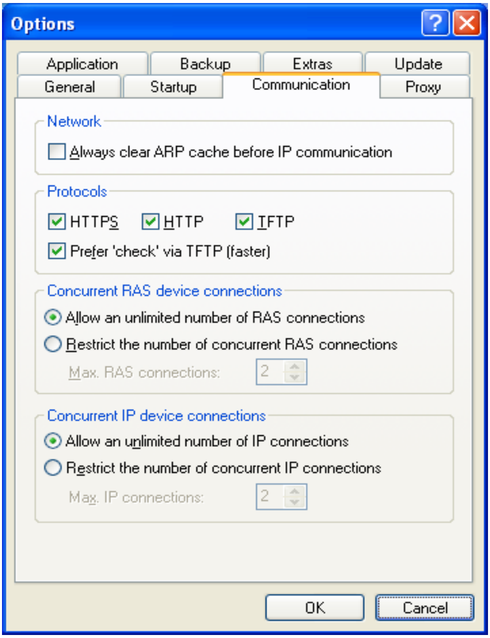
With LANconfig, device actions are typically conducted using the tftp protocol. Because this protocol has disadvantages compared to other protocols when transmitting large volumes of data, the protocols https and http can be used as alternatives.

The use of protocols can be set either globally for all devices managed by a LANconfig or specifically for each individual device. The global settings overwrite the local settings—thus when device-specific settings are selected, those settings take effect exclusively if they are also selected globally.

1.12.1 Global Settings for Communication Protocols

When setting up the communications protocols, differentiate between the protocol that is used solely for checking the device, and protocols used for other operations such as a firmware upload, etc.

To access and configure global communication settings, open the following dialog: `Tools : Options : Communication`



Network

□ Always clear ARP cache before IP communication

Protocols

☑ HTTPS ☑ HTTP ☑ TFTP

☑ Prefer 'check' via TFTP (faster)

Concurrent RAS device connections

● Allow an unlimited number of RAS connections

○ Restrict the number of concurrent RAS connections

Max. RAS connections: 2

Concurrent IP device connections

● Allow an unlimited number of IP connections

○ Restrict the number of concurrent IP connections

Max. IP connections: 2

The following global communication settings can be configured:

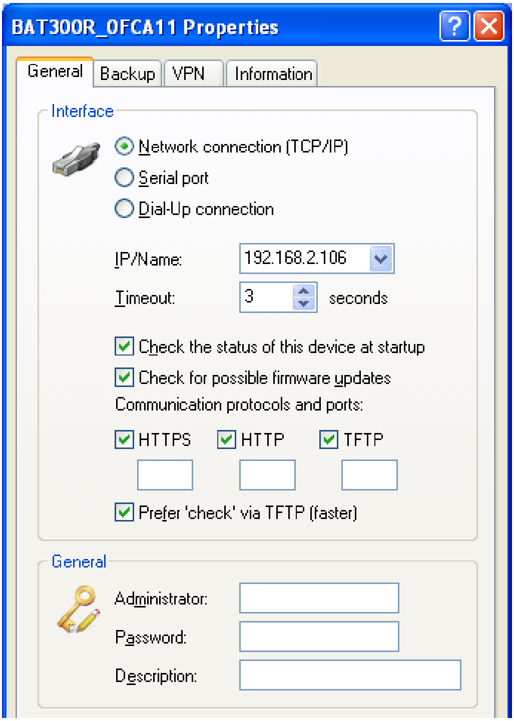
- https, http, tftp:
  When this is selected, the individual protocols are enabled for the operations firmware upload, configuration up/download, and script up/download. During these operations, LANconfig attempts to use these protocols in the order https, http and tftp. If the transfer cannot be performed using a selected protocol, then the next protocol is automatically attempted.
- Prefer checks via tftp:
  When checking the devices, small amounts of data are transferred with the system information. As such, device checks could be performed using the tftp protocol, particularly in the LAN. When this option is activated, the tftp protocol is used to check the device first, regardless of the previously set communications protocols. If the check via tftp cannot be performed, then the protocols https, http and tftp are attempted in that order.

1.12.2 Device-Specific Settings for Communication Protocols

The device-specific settings are subordinate to the global communications settings. This lets you restrict a protocol centrally for the entire project. When multiple protocols are selected, LANconfig attempts to establish communications using protocols in the following sequence: https, http and tftp.

To access and configure device-specific communication settings for a selected device in LANconfig, follow these steps:

- □ In LANconfig, select a device in the list, click the right mouse button, and select ‘Properties’.
- □ Open the ‘General’ tab of the ‘Options’ dialog:



Interface

● Network connection (TCP/IP)
○ Serial port
○ Dial-Up connection

IP/Name: 192.168.2.106
Timeout: 3 seconds

☑ Check the status of this device at startup
☑ Check for possible firmware updates

Communication protocols and ports:
☑ HTTPS ☑ HTTP ☑ TFTP

☑ Prefer 'check' via TFTP (faster)

General

Administrator:
Password:
Description:

The following device-specific communication settings can be configured:

- https, http, tftp:
  Select the communications protocols as described in the global settings. In the fields under the protocols, you can specify the port to be used for that protocol. The following default port settings are used if these fields are left blank, or if a value of ‘0’ is entered:
  - https: port 443
  - http: port 80
  - tftp: port 69
- Prefer checks via tftp:
  Preferred checking via tftp as described in the global settings.

  Note: For all specific communications settings, the global settings take priority. A protocol can therefore exclusively be used for operating a device when it is also activated in the global settings.

1.13 Exporting CSV data sets

You export the list of devices found in the network so that you can conveniently import them back into LANconfig later on in one operation. You have the option to export the list of managed devices as a CSV file.
To export the data, you proceed as follows:

□ In the menu, choose `File:Export device list`.

□ Specify the storage location for the file.

□ Enter a file name.

□ Specify the column separator with which you separate the respective device parameters.

□ To start the exporting of the file, click “Save”.

□ A dialog confirms the number of saved device data sets.

□ Click “OK” to close this dialog.

The CSV file created contains the following data:

```
DEVICE_PATH;DEVICE_INTERFACE;DEVICE_ADDRESS;DEVICE_TIMEOUT;DEVICE_STA
RTUP;DEVICE_PROTOCOLS;DEVICE_PORTS;DEVICE_ADMIN;DEVICE_PASSWORD;DEVIC
E_NAME;DEVICE_DESCRIPTION;DEVICE_TYPE;DEVICE_SERNO;DEVICE_HWADDR;DEVI
CE_HWREL;DEVICE_LOCATION;DEVICE_COMMENT;DEVICE_BACKUP;DEVICE_VPNGrupp
e1;IP;192.168.2.35;10;1;263;;admin;Ht34bd5L;Etage1;<Gerätename>;Hirsc
hmann <Gerätename>
Wireless;008520600482;00a0570bc9bf;B;;;;Gruppe1;IP;192.168.2.34;10;1;
263;;admin;Ht34bd5L;Etage2;L-54ag;HirschmannL-54ag
Wireless;008520600843;00a05719a8fb;B;;;;
```

The 1st line contains names of the device parameters, and under this a line appears for each device with the corresponding parameter values. If 2 semi-colons appear directly in sequence, the enclosed parameter value is empty.
The variable names of the 1st line correspond to the following LANconfig entries:

- `DEVICE_PATH`: Path name in the folder view
- `DEVICE_INTERFACE`: Connection type
- `DEVICE_ADDRESS`: IP address or domain name and COM port or telephone number
- `DEVICE_TIMEOUT`: Maximum response time of the device
- `DEVICE_STARTUP`: Device checking during startup

- `DEVICE_PROTOCOLS`: Communication protocols
- `DEVICE_PORTS`: Ports
- `DEVICE_ADMIN`: Administrator name
- `DEVICE_PASSWORD`: Administrator password
- `DEVICE_NAME`: Device name
- `DEVICE_DESCRIPTION`: Description
- `DEVICE_TYPE`: Device type
- `DEVICE_SERNO`: Serial number
- `DEVICE_HWADDR`: MAC address
- `DEVICE_HWREL`: Hardware release
- `DEVICE_LOCATION`: Location where used
- `DEVICE_COMMENT`: Comment
- `DEVICE_BACKU` : Storage location of configuration backup created by LANconfig
- `DEVICE_VPN`: Parameter set for 1-click VPN

Note: You have the option of editing the list of exported devices with a text editor or, more conveniently, in a table calculation.

Note: If you have stored access data for a device in the LANconfig, then LANconfig stores the password unencrypted in the CSV file. Therefore, delete the access data in the file before forwarding it or storing it on a freely accessible server.

1.13.1 Enhancements in the menu system

- File
  Under the ‘File’ menu item you can manage devices generally and finish LANconfig.
- Exporting the device list
  You export the list of devices found in the network so that you can conveniently import them back into LANconfig later on in one operation. You then have the option to export the list of devices managed in LANconfig as a CSV file.

1.14 Importing from a data source

You import a large number of devices into LANconfig from a script template in one operation by loading a corresponding device file using an import wizard. You can also use this device file and a configuration template file to create an individual configuration file for each device. The template file contains variables that contain the values of the device file.

Note: The device file is stored in the CSV format.

1.14.1 Enhancements in the menu system

- File
  - Under the ‘File’ menu item you can manage devices generally and finish LANconfig.
- Devices/configurations from CSV file...
  - You import a large number of devices into LANconfig from a script template in one operation by loading a corresponding device file using an import wizard. You can also use this device file and a configuration template file to create an individual configuration file for each device. The template file contains variables that store the values of the device file.

1.14.2 Application example for importing from a data source

This scenario describes how you use a general script file and a simple CSV device file to create your data source for the data import.

- **Content of the CSV file**
  The CSV file contains data sets of devices. You can import these into LANconfig in order to manage them conveniently in the network.
  A simple CSV file looks like this, for example:

  ```
  CONFIG_FILENAME;DEVICE_PATH;DEVICE_INTERFACE;DEVICE_A
  DDRESS;DEVICE_LOCATION;DEVICE_NAME;KEY;USERFil52146.l
  cs;Filialen/
  NRW;IP;192.168.1.1;Neckertenzlingen;Fil52146;secret1;
  user1@internetFil80637.lcs;Filialen/
  BAY;IP;192.168.2.1;Muenchen;Fil80637;secret2;user2@in
  ternet
  ```

  The title line contains the names of the device parameters. Below this the individual devices are listed line by line, with their parameters separated from each other by semi-colons. If 2 semi-colons appear directly in sequence, the enclosed parameter value is empty.
  You can enter any values for the names of the parameters in the 1st line. Use the available Hirschmann standard variable names so that LANconfig automatically assigns the device parameters when importing:

- DEVICE_PATH: Path name in the folder view
- DEVICE_INTERFACE: Connection type
- DEVICE_TIMEOUT: Maximum response time of the device
- DEVICE_STARTUP: Device checking during startup
- DEVICE_PROTOCOLS: Communication protocols
- DEVICE_PORTS: Ports
- DEVICE_ADMIN: Administrator name
- DEVICE_PASSWORD: Administrator password
- DEVICE_NAME: Device name
- DEVICE_DESCRIPTION: Description
- DEVICE_BACKUP: Storage location of configuration backup created by LANconfig
- DEVICE_VPN: Parameter set for 1-click VPN

If you do not use Hirschmann standard variable names, then you assign the values to the corresponding device properties in LANconfig during the import, if applicable.

- **Content of the configuration template file**
  The template file contains commands that Telnet executes in sequence. This is why the template file is also known as the “script file”.

  Note: You will find an overview of the available Telnet commands in the reference manual, chapter “Configuration with Various Tools”, under “Telnet”.

  A configuration template file looks like this, for example:

```
lang English
flash No
set /Setup/Name "$DEVICE_NAME$"
set /Setup/SNMP/Location "$DEVICE_LOCATION$"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID
Interface Src-check Type Rtg-tag Comment
add "INTRANET" $DEVICE_ADDRESS$ 255.255.255.0 0 any
loose Intranet 0 "local intranet"
cd /
cd /Setup/WAN/PPP
```

```
tab Peer Authent.request Authent-response Key Time Try
Conf Fail Term Username Rights
add "INTERNET" none PAP "$KEY$" 6 5 10 5 2 "$USER$" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI
ATM-VCI MAC-Type user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOE" 1 32 local
000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance
Masquerade Active Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes
"default route"cd /
flash Yes

# done
exit
```

The variables start and end with a character or a character string (here: ‘$’).

In this template file, the variables represent specific device parameters. During the import procedure, you link these variables with the corresponding entries in the device file. The configuration wizard then replaces the variables with the assigned device data from the CSV file.

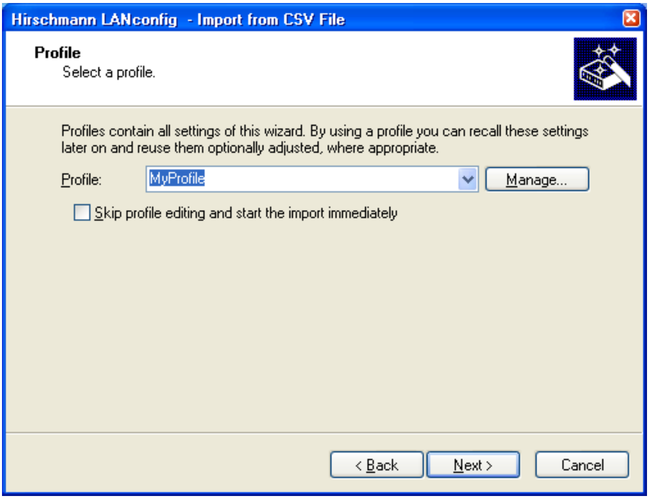
▶ **Creating configuration files**

You create device-specific configuration files as follows:

☐ Open the import wizard in the menu via `File:Devices/configurations from CSV file...`

☐ Confirm the welcome dialog with “Continue”, if applicable. The option “Skip this page next time” hides the welcome dialog when you call up the wizard in the future.

☐ If applicable, select the saved profile of a previous data import. To copy the settings of the selected profile without any changes, activate the option “Skip profile editing and start the import immediately”. To create a new profile, select “New profile”. Click “Next”.



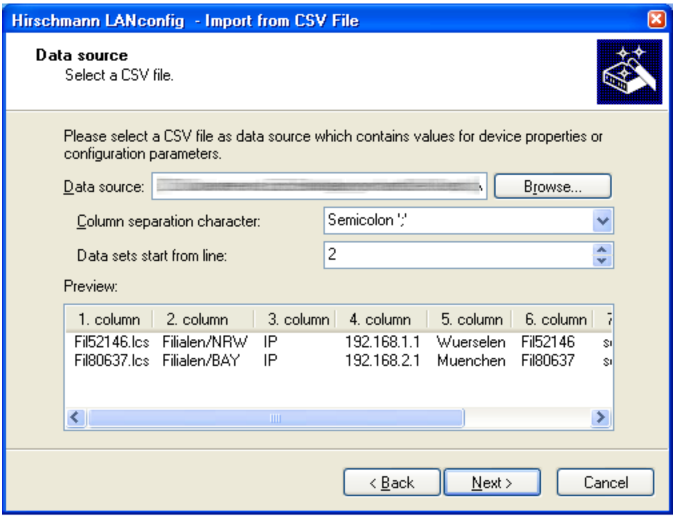
Profiles contain all settings of this wizard. By using a profile you can recall these settings later on and reuse them optionally adjusted, where appropriate.

Profile: MyProfile

□ Skip profile editing and start the import immediately

Figure 20: New profile for importing a CSV file

□ Enter the path for the CSV file in the “Data source” field. With “Browse...” you look for this file in the local file system.



Data source

Select a CSV file.

Please select a CSV file as data source which contains values for device properties or configuration parameters.

Data source: [redacted] Browse...

Column separation character: Semicolon ';'

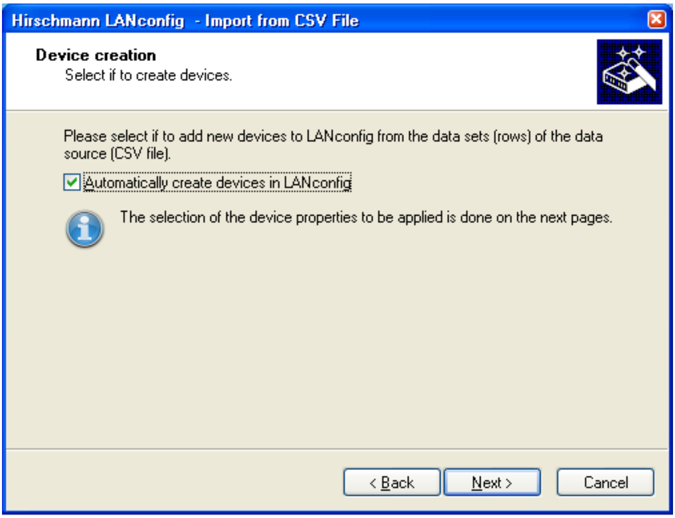
Data sets start from line: 2

Preview:

1. column	2. column	3. column	4. column	5. column	6. column	7
Fil52146.lcs	Filialen/NRW	IP	192.168.1.1	Wuerselen	Fil52146	s
Fil80637.lcs	Filialen/BAY	IP	192.168.2.1	Muenchen	Fil80637	s

Figure 21: Select the data source for the CSV file

- ☐ Specify the character to be used as a column separator in the CSV file. The default setting is a semi-colon.
- ☐ Specify from which line the data sets start and thus exclude and column titles that may exist and any additional information from the import. If a line in the CSV file only contains Hirschmann standard variable names (see section “Exporting CSV data sets”), LANconfig uses this line for the automatic assignment of the variables. This ensures that an export and the importing of the same file works without manual assignment. If you add variables for the creation of the configuration, there is no auto-detection.
- ☐ The “Preview” field immediately displays the data sets to be imported based on your selected parameters. Confirm your entry with “Next”.
- ☐ To create new devices in LANconfig using the data sets, you activate the option “Automatically create devices in LANconfig”. When you click “Next”, the following screens enable you to select the device properties that you want to copy to LANconfig.



Hirschmann LANconfig - Import from CSV File

Device creation

Select if to create devices.

Please select if to add new devices to LANconfig from the data sets (rows) of the data source (CSV file).

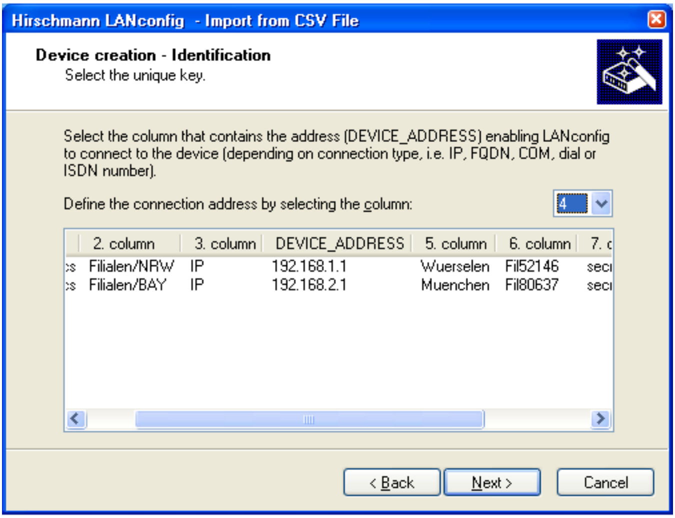
☑ Automatically create devices in LANconfig

The selection of the device properties to be applied is done on the next pages.

Figure 22: Selecting device properties to be copied

☐ If the option is deactivated, the wizard skips the next 2 steps.

The devices are identified using the connection address. In the drop-down list, select the column of the data set that contains the connection address, then click “Next”. When the Hirschmann standard variable names are being used, this assignment is performed automatically.



Device creation - Identification

Select the unique key.

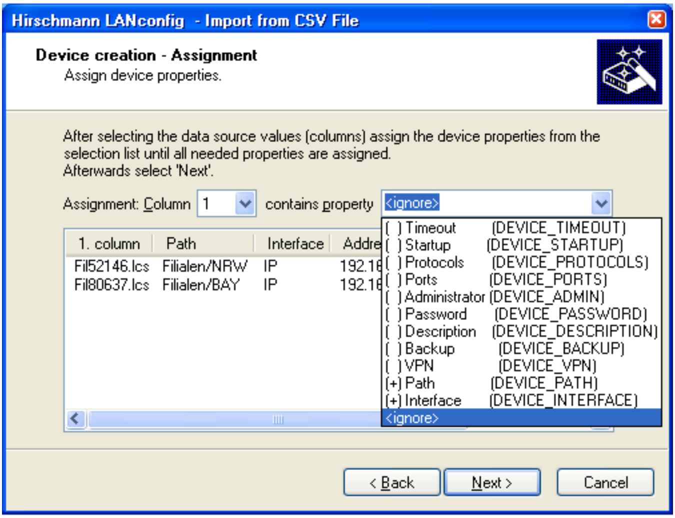
Select the column that contains the address (DEVICE_ADDRESS) enabling LANconfig to connect to the device (depending on connection type, i.e. IP, FQDN, COM, dial or ISDN number).

Define the connection address by selecting the column: 4

	2. column	3. column	DEVICE_ADDRESS	5. column	6. column	7. c
:s	Filialen/NRW	IP	192.168.1.1	Wuerselen	Fil52146	seci
:s	Filialen/BAY	IP	192.168.2.1	Muenchen	Fil80637	seci

Figure 23: Selecting the connection address for identification

☐ Assign the columns to the device properties. The prefixed “+” indicates the assigned properties in the list. Now click “Next”. When the Hirschmann standard variable names are being used, this assignment is performed automatically.



Hirschmann LANconfig - Import from CSV File

Device creation - Assignment

Assign device properties.

After selecting the data source values (columns) assign the device properties from the selection list until all needed properties are assigned.
Afterwards select 'Next'.

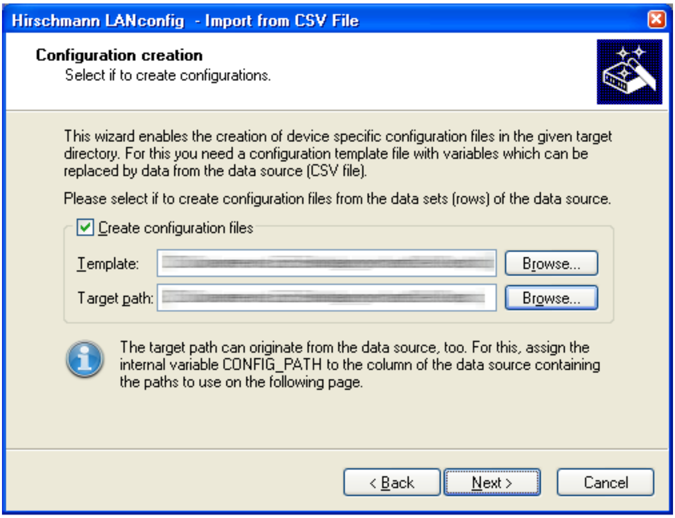
Assignment: Column 1 contains property <ignore>

1. column	Path	Interface	Addre
Fil52146.lcs	Filialen/NRW	IP	192.16
Fil80637.lcs	Filialen/BAY	IP	192.16

( ) Timeout (DEVICE_TIMEOUT)
( ) Startup (DEVICE_STARTUP)
( ) Protocols (DEVICE_PROTOCOLS)
( ) Ports (DEVICE_PORTS)
( ) Administrator (DEVICE_ADMIN)
( ) Password (DEVICE_PASSWORD)
( ) Description (DEVICE_DESCRIPTION)
( ) Backup (DEVICE_BACKUP)
( ) VPN (DEVICE_VPN)
(+) Path (DEVICE_PATH)
(+) Interface (DEVICE_INTERFACE)
<ignore>
< Back
Next >
Cancel

Figure 24: Assignment of the device properties

☐ To create individual configuration files from the data records, activate the option “Create configuration files”.



Hirschmann LANconfig - Import from CSV File

Configuration creation

Select if to create configurations.

This wizard enables the creation of device specific configuration files in the given target directory. For this you need a configuration template file with variables which can be replaced by data from the data source (CSV file).

Please select if to create configuration files from the data sets (rows) of the data source.

☑ Create configuration files

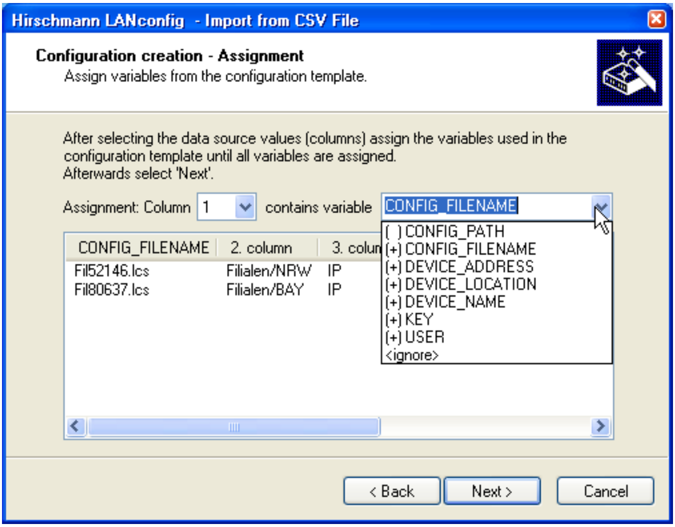
Template:

Target path:

The target path can originate from the data source, too. For this, assign the internal variable CONFIG_PATH to the column of the data source containing the paths to use on the following page.

Figure 25: Creating a configuration file

- □ In the “Template” field you specify the path of the template file to be used as a basis for the individual configuration files. Click “Browse...” to open the dialog for loading a configuration script template. In the “Variable start” and “Variable end” fields you define the characters (or character strings) with which the variables in the template file start and end. The wizard thus identifies the variables in the template file.
- □ In the “Target path” field you specify where LANconfig saves the new configuration files. Click “Browse...” to define the target path in the local file system. Click “Next”.
- □ Assign the variables used in the template file to the columns of the data source. To do this, select the column number from the column list and assign a variable from the variable list to this number. If the column title contains the same variable names that you entered in the script between the start and end characters, an automatic assignment is also carried out for all the variables found. The column titles in the view below this are immediately refreshed for every change. Now click “Next”.



Hirschmann LANconfig - Import from CSV File

Configuration creation - Assignment

Assign variables from the configuration template.

After selecting the data source values (columns) assign the variables used in the configuration template until all variables are assigned.
Afterwards select 'Next'.

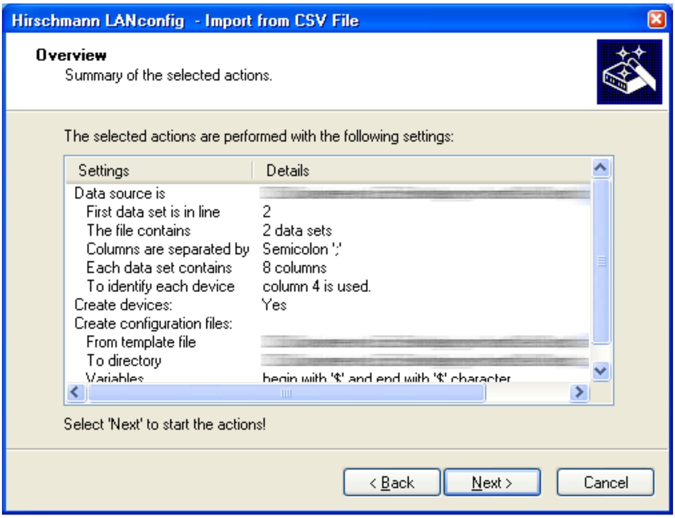
Assignment: Column 1 contains variable CONFIG_FILENAME

CONFIG_FILENAME	2. column	3. colun
Fil52146.lcs	Filialen/NRW	IP
Fil80637.lcs	Filialen/BAY	IP

Figure 26: Assigning the variables for the template file

□ If your entries are incomplete, the wizard informs you about possible problems with the importing and offers you corrections.

□ The summary shows you what actions are performed in the next step. To make changes , click “Back”. The corresponding input screen appears. Click “Next” to start the data import.
If the data import would overwrite a device that already exists in LANconfig, the wizard presents you with the following options to choose from:



Overview

Summary of the selected actions.

The selected actions are performed with the following settings:

Settings	Details
Data source is	[redacted]
First data set is in line	2
The file contains	2 data sets
Columns are separated by	Semicolon ';'
Each data set contains	8 columns
To identify each device	column 4 is used.
Create devices:	Yes
Create configuration files:	
From template file	[redacted]
To directory	[redacted]
Variables	begin with '$' and end with '$' character

Select 'Next' to start the actions!

Figure 27: Start data import

□ The subsequent status dialog shows which actions have been performed. You click “Copy to clipboard” to save the status message in the clipboard. Click “Next”.

□ To finish, you have the option of saving the current import settings in a profile for future actions.

□ End the import by clicking “Finish”.

▶ **Creating configuration files**

If you selected the creation of an individual configuration file, then the wizard has created a separate configuration file for each device in the CSV file for the specified folder. This has the file name defined in the CSV file: “<CONFIG_FILENAME>.lcs”:

```
lang English
flash No
set /Setup/Name "Fil52146"
set /Setup/SNMP/Location "Neckartenzlingen"
cd /Setup/TCP-IP/Network-list
tab Network-name IP-Address IP-Netmask VLAN-ID
Interface Src-check Type Rtg-tag Comment
add "INTRANET" 192.168.1.1 255.255.255.0 0 any loose
```

```
Intranet 0 "local intranet"
cd /
cd /Setup/WAN/PPP
tab Peer Authent.request Authent-response Key Time Try
Conf Fail Term Username Rights
add "INTERNET" none PAP "secret1" 6 5 10 5 2
"user1@internet" IP
cd /
cd /Setup/WAN/DSL-Broadband-Peers
del *
tab Peer SH-Time AC-name Servicename WAN-layer ATM-VPI
ATM-VCI MAC-Type user-def.-MAC DSL-ifc(s) VLAN-ID
add "INTERNET" 9999 "" "" "PPPOEOA" 1 32 local
000000000000 "" 0
cd /
cd /Setup/IP-Router/IP-Routing-Table
tab IP-Address IP-Netmask Rtg-tag Peer-or-IP Distance
Masquerade Active Comment
add 255.255.255.255 0.0.0.0 0 "INTERNET" 0 on Yes
"default route"
cd /
flash Yes

# done
exit
```

The wizard has replaced all the variables with the corresponding device data.

Use this configuration file to transfer the device settings defined with the template file to other devices in LANconfig. To do this, select the corresponding device and click `Device:Configuration Management:Restore Script from File`.

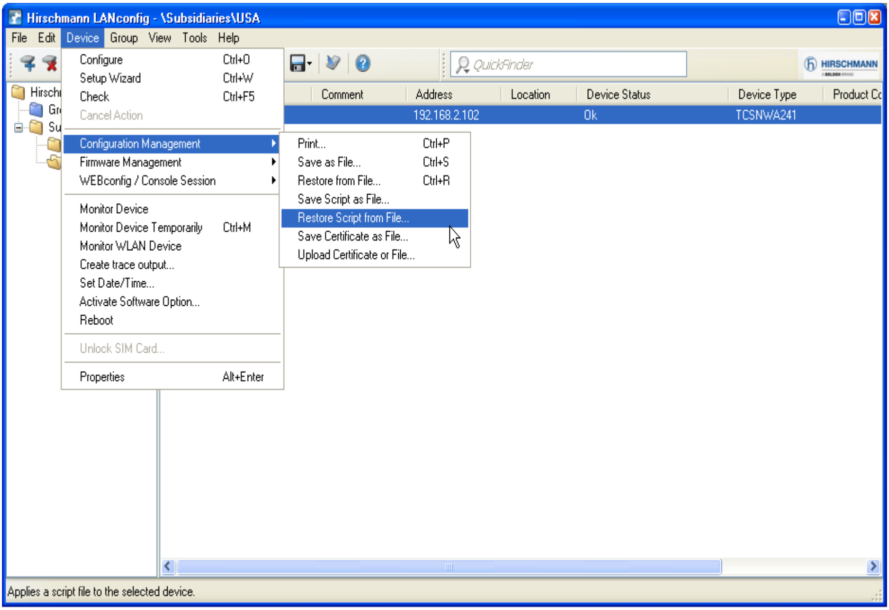


Figure 28: Transferring device properties from configuration file

2 Connecting to the Device

Before you can operate and manage the OpenBAT device, set up a connection to the device. To do this, you have to identify the IP address of the device, among other things.

2.1 Identifying the specified IP address

The IP address initially assigned to the OpenBAT device depends on where the device is connected when it is first switched on. Example:

- When the OpenBAT device is physically connected with a private network of class C (e.g. 192.168.100.0/255.255.255.0), there are two possible scenarios:
  - The network contains an active DHCP (Dynamic Host Configuration Protocol) server. Then the OpenBAT device behaves like a DHCP client and gets its IP address from the DHCP server.
  - The network does not contain a DHCP server, and none of the existing data network devices is a DHCP client. In this case, the IP addresses are assigned statically. The OpenBAT device then takes over the general network address of the static devices (e.g. 192.168.100.x) and adds the value 254 as the fourth object. In this example, the OpenBAT device would have the IP address “192.168.100.254”.

  Note: In the above scenario, the OpenBAT device is connected to a single configuration PC that has a static IP address. The device takes over the network address of the configuration PC and adds “254” as the fourth byte.

- When the OpenBAT device in a network without a DHCP server is connected with other devices that are all acting as DHCP clients, the OpenBAT device activates its own DHCP server and assigns IP addresses to all the devices, including itself. In this case, the OpenBAT device assigns the general network address 172.23.56.x to all the devices, and the fourth byte 254 to itself. Then its IP address would be “172.23.56.254”.

  Note: The above scenario also applies to devices that are connected with a single configuration PC that is configured as a DHCP client.

To simplify the first connection setup to the OpenBAT device, connect the device to the configuration PC only.

2.2 Making the Initial Connection

The following section tells you how to set up the first connection to the OpenBAT device. For this you require a configuration PC, the OpenBAT device, a voltage source for the OpenBAT device and an Ethernet cable.

Before you start, familiarize yourself with the following requirements:

- The configuration PC is connected to the OpenBAT device by means of the Ethernet cable only. Do not set up any other data network connections to these devices.
- Carry out this procedure on one OpenBAT device, not on multiple devices at the same time.
- The configuration PC is configured in such a way that it gets an IP address from the DHCP server.
- The factory settings of the OpenBAT device are the standard parameters. To set up this basic configuration, press the reset button on the OpenBAT for 6 seconds before you start setting up the connection.

2.2.1 Connection Procedure

This is how you set up a connection between the configuration PC and the OpenBAT device:

☐ Make sure that both devices are disconnected from the voltage source. Plug the Ethernet cable into the PC and the OpenBAT device. Make sure that there are no other Ethernet connections to the devices.

☐ Connect the OpenBAT device to the voltage source. For more information on terminal block wiring see the "Installation user manual OpenBAT family".

□ When the Power LED and the LED to the right of it on the OpenBAT device are flashing green or green/orange, hold down the reset button for five seconds with a pointed object (e.g. an opened paper clip or a small screwdriver) (see page 115). When the LEDs on the device are lit continuously in red, release the reset button.

□ Once the LEDs on the OpenBAT device are flashing green or green/orange again, switch on the PC. Within a few seconds, the WiFi devices assigns an IP address for networks of class C to the PC. The IP address begins with the bytes “172.23.56”.

□ In order to see your computer’s IP address, open a command prompt window, type ‘ipconfig’, and push ‘Enter’. The window displays the IP address for the local area connection that you have just made, starting with 172.23.56. (Other IP addresses may be also displayed, but you are interested in just the one associated with this local area connection.)

□ Open a web browser on your computer. In the address window of the browser, enter the first three octets of your computer’s IP address (172.23.56), and use 254 as the fourth octet (172.23.56.254).

Note:

▶ The IP address that you use for the OpenBAT device (172.23.56.254) is only used for the initialization of the device. During the device configuration, assign the WiFi device either a new unique IP address, or configure the device so that when it is setting up a connection with the network, it gets an IP address from the server.

▶ If you configure multiple devices with the same IP address, it's possible that unforeseen functions will be triggered in the network.

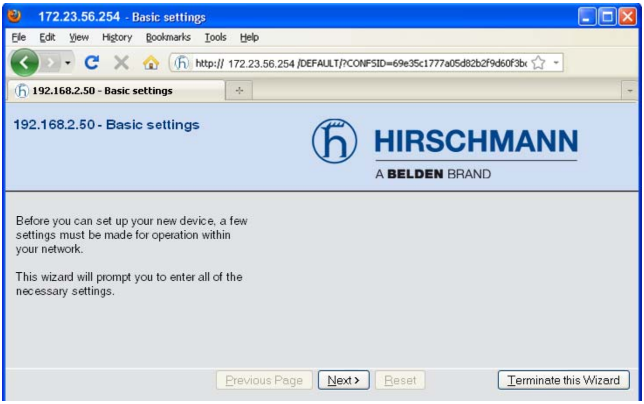
⚠ WARNING

UNINTENTIONAL OPERATION IN DEVICE

Install and maintain a process that assigns a unique IP address to every device in the network.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

The following page opens:



172.23.56.254 - Basic settings
File
Edit
View
History
Bookmarks
Tools
Help
http:// 172.23.56.254 /DEFAULT/?CONFSID=69e35c1777a05d82b2f9d60f3b
192.168.2.50 - Basic settings
HIRSCHMANN
A BELDEN BRAND
Previous Page
Next >
Reset
Terminate this Wizard

192.168.2.50 - Basic settings

Before you can set up your new device, a few settings must be made for operation within your network.

This wizard will prompt you to enter all of the necessary settings.

You are now connected with the first web page of the OpenBAT device. You can configure the device as follows:

- using the device web pages, beginning with the first page of the setup wizard (above), or
- running the LANconfig software provided on the distribution CD.

Note: The IP address of the OpenBAT device (with “254” as the last byte) is only used to initialize the device. During the device configuration, assign the OpenBAT device either a new unique IP address, or configure the device so that when it is setting up a connection with the network, it gets an IP address from the server.

3 Upload Settings to the Device

As soon as a connection is set up to the new OpenBAT device (see page 77), you have the option of loading pre-configured settings onto the device. These pre-configured settings can be found in the following form:

- as a configuration file (suffix “.lcf”):
  You either create this file yourself using LANconfig, or you transfer the existing settings from a OpenBAT device using one of the following procedures:
  - with the LANconfig program: Select a device, then choose the following options: `Device : Configuration Management : Save as file`
  - with the WEBconfig program: Navigate to a device, then choose the following options:

🟦 `File Management : Saving a configuration`

Note: You will find the instructions for creating, editing and saving configuration files in the OpenBAT Configuration and Administration Guide.

- as a configuration file (suffix “.lcf”):
  You either create this file yourself using a text editor, or you load the existing settings from a OpenBAT device using one of the following procedures:
  - with the LANconfig program: Select a device, then choose the following options: `Device : Configuration Management : Save as script file`
  - with the WEBconfig program: Navigate to a device, then choose the following options:

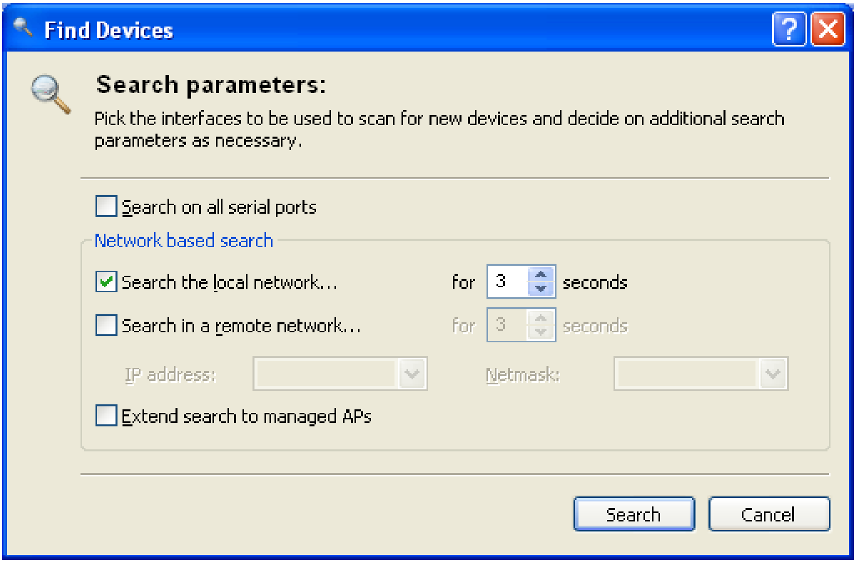
■ `File Management : Save configuration script`

3.1 Uploading Settings in LANconfig

To upload a configuration or script file using the LANconfig software, follow these steps:

☐ Install and start-up the LANconfig software that is provided on the distribution CD.

☐ Find the OpenBAT device using LANconfig. Select `File : Find Devices`. The “Find Devices” dialog opens:



Find Devices

Search parameters:

Pick the interfaces to be used to scan for new devices and decide on additional search parameters as necessary.

☐ Search on all serial ports

Network based search

☑ Search the local network... for 3 seconds

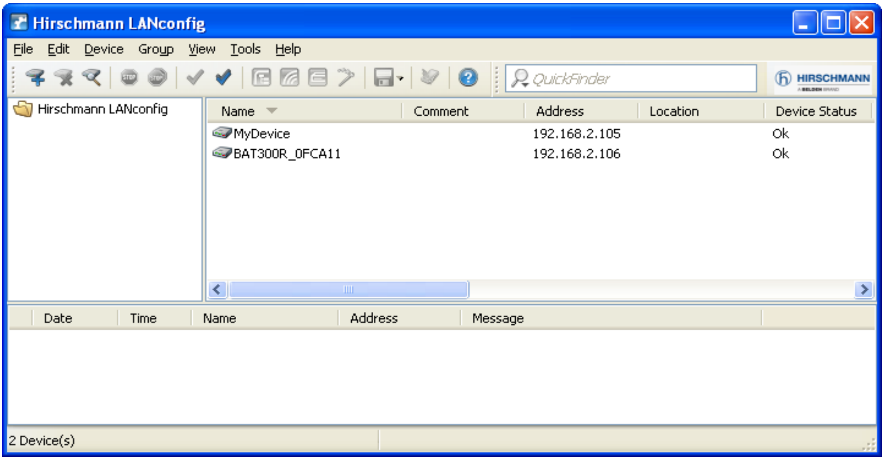
☐ Search in a remote network... for 3 seconds

IP address: Netmask:

☐ Extend search to managed APs

☐ Click ‘OK’.

LANconfig searches for devices on the network, then displays the discovered device(s) in the LANconfig software:



Name	Comment	Address	Location	Device Status
MyDevice		192.168.2.105		Ok
BAT300R_0FCA11		192.168.2.106		Ok

2 Device(s)

□ If LANconfig starts the setup wizard, click ‘Cancel’ to end the wizard configuration process. If prompted, click ‘Yes’ to confirm the cancellation of the wizard and return to the LANconfig main window

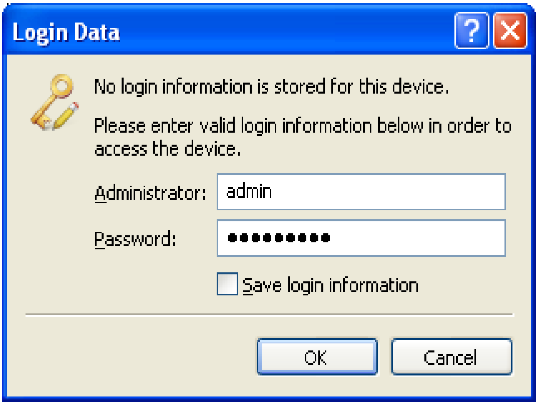
□ In the list of devices found, select the device to which you want to transfer the settings.

□ After you've selected the targeted device, perform one of the following steps:

- ▶ To load the settings from a configuration file, choose one of the following options: `Device : Configuration Management : Restore from file`
- ▶ To load the settings from a configuration script, choose one of the following options: `Device : Configuration Management : Restore Script from File`

Note: Choose the configuration or script file which is pre-configured for a device conforming to the type and firmware version of your current device.

□ If LANconfig asks for a password, input the password for the device.



No login information is stored for this device.

Please enter valid login information below in order to access the device.

Administrator: admin

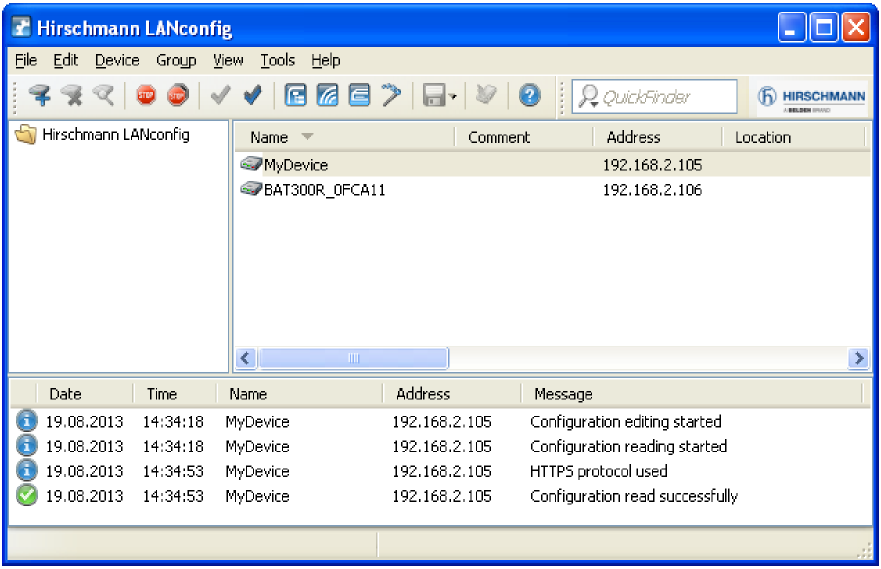
Password: ●●●●●●●●●●

□ Save login information

Note: The default password is `private`. Do not enter a value in the ‘Administrator‘ field.

□ In the file selection dialog, navigate to and select the configuration file or script to apply to the selected device, then click ‘Open’.

The LANconfig software applies the new settings and displays the following information when complete:



Name	Comment	Address	Location
MyDevice		192.168.2.105	
BAT300R_0FCA11		192.168.2.106	

Date	Time	Name	Address	Message
19.08.2013	14:34:18	MyDevice	192.168.2.105	Configuration editing started
19.08.2013	14:34:18	MyDevice	192.168.2.105	Configuration reading started
19.08.2013	14:34:53	MyDevice	192.168.2.105	HTTPS protocol used
19.08.2013	14:34:53	MyDevice	192.168.2.105	Configuration read successfully

Note: The new settings include a different IP address. The device can no longer be reached using the original IP address.

3.2 Uploading Settings in WEBconfig

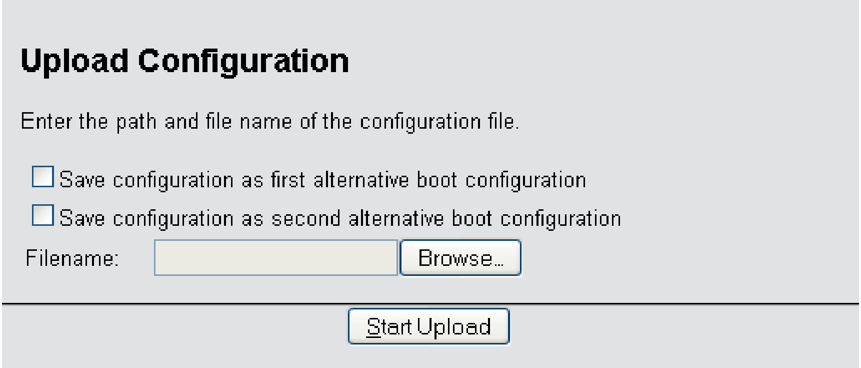
To upload a configuration or script file using WEBconfig, follow these steps:

□ Use WEBconfig to set up a first connection to the OpenBAT device (see page 79).

▶ To upload a configuration file, select the following options:

`File management : Upload Configuration`

The following dialog opens:



Upload Configuration

Enter the path and file name of the configuration file.

□ Save configuration as first alternative boot configuration

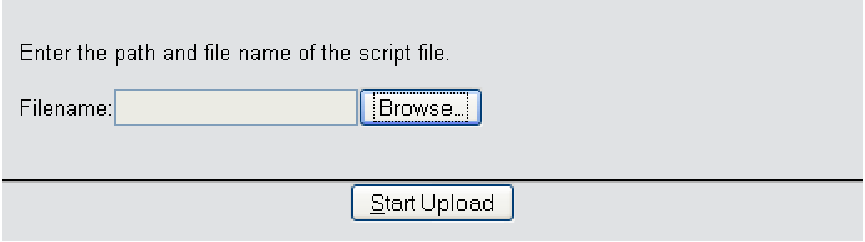
□ Save configuration as second alternative boot configuration

Filename:

▶ To upload a script file, select:

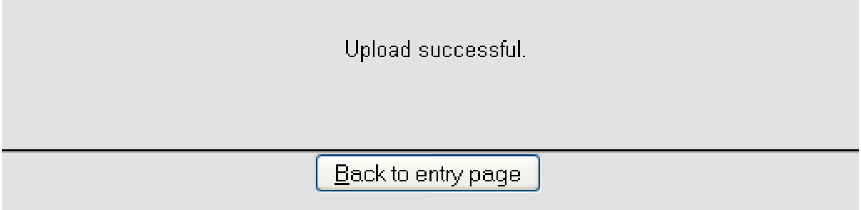
🟦 `File management : Execute Configuration Script`

The following dialog opens:



Enter the path and file name of the script file.

- □ Click the ‘Browse’ button, to open a ‘File Upload’ dialog.
- □ Navigate to and select the configuration or script file to execute, then click ‘Open’.
- □ Click “Start Upload”. After the upload is finished, WEBconfig displays the following dialogue:



Upload successful.

Note: Remember that the new settings include a different IP address. The device can no longer be reached using the original IP address.

4 Working with Device Files

4.1 Creating, Editing and Uploading Files

Both the LANconfig and the WEBconfig software let you work with configuration (.lcf) files and script (.lcs) files.

Note: You can upload a saved configuration file to a device that is the same type and with the same firmware version as defined in the configuration file.

4.1.1 Creating, editing and printing files in LANconfig

LANconfig allows you to perform the following tasks:

- to create a new configuration file (.lcf) for the OpenBAT device and save it on the configuration PC. For this you use the command `Edit : New Configuration File`.
- to edit a saved configuration file on the PC. For this you use the command `Edit : Edit Configuration File`.
- to open the setup wizard and edit a saved configuration file on the PC. For this you use the command `Edit : New Configuration File`
- to print the selected file with the configuration settings. For this you use the command `Edit : New Configuration File`

4.1.2 Uploading and Downloading Device Files

Using either LANconfig or WEBconfig, you can:

- Download a device’s configuration settings to an.lcf file on your configuration PC:
  `Device : Configuration Management : Save as file`

  🟦 `File Management : Saving a configuration`

- Upload a saved configuration (.lcf) file to a selected device:
  `Device : Configuration Management : Restore from file`

  🟦 `File Management : Saving a configuration`

- Download a device’s settings to an script (.lcs) file on your configurationPC:
  `Device : Configuration Management : Save as script file`

  🟦 `File Management : Save configuration script`

- Upload a saved script (.lcs) file to a selected device:
  `Device : Configuration Management : Restore Script from File`

  🟦 `File Management : Restore Script from File`

- Download a device certificate to a file on your configuration PC:
  `Device : Configuration Management : Save Certificate Save as File`

  🟦 `File Management : Download Certificate or File`

- Upload a saved certificate file to a selected device:
  `Device : Configuration Management : Upload Certificate or File`

  🟦 `File Management : Upload Certificate or File`

4.2 Automatic Backup of Files in LANconfig

LANconfig can automatically save backups of the current configuration prior to changes in firmware or configuration. LANconfig can be configured to perform this task either globally for all devices, or for selected devices.

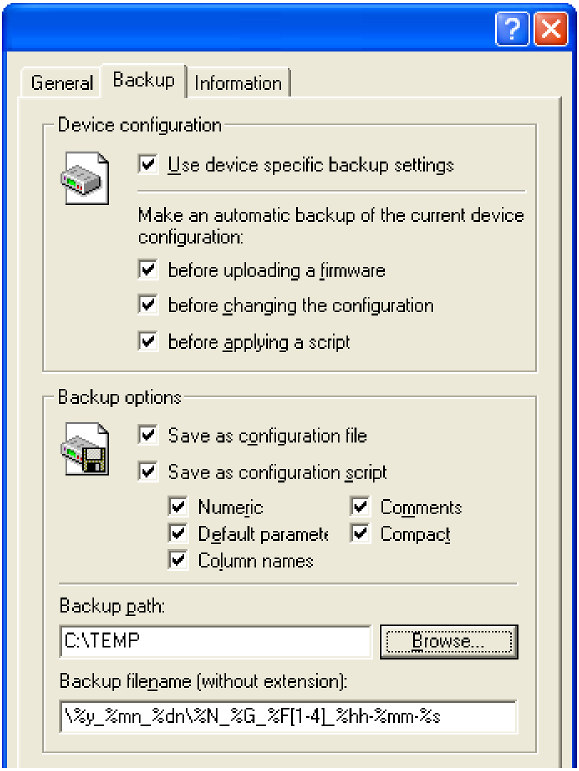
To configure global automatic configuration file backup for all devices:

☐ In LANconfig, select `Tools : Options`, then click the ‘Backup’ tab to open that dialog.

To configure automatic configuration file backup for a specific devices:

☐ In LANconfig, select the specific device to configure, and click the right mouse button.

☐ From the pop-up menu select `Properties`, then click the ‘Backup’ tab to open the following dialog:



Device configuration

☑ Use device specific backup settings

Make an automatic backup of the current device configuration:

☑ before uploading a firmware

☑ before changing the configuration

☑ before applying a script

Backup options

☑ Save as configuration file

☑ Save as configuration script

☑ Numeric ☑ Comments

☑ Default paramete ☑ Compact

☑ Column names

Backup path:

C:\TEMP

Backup filename (without extension):

\%y_%mn_%dn\%N_%G_%F[1-4]_%hh-%mm-%s

Select the desired automatic file backup settings in these dialogs, including the following:

- Select ‘Use device-specific backup settings’ (in the device-specific dialog) and the automatic backup settings made in the device configuration will override the global settings.
- Select one or more events, prior to which the configuration is to be saved:
  - firmware upload
  - configuration change
  - script execution
- Select the formats in which the configuration is to be saved (configuration file, script - possibly with options).
  - configuration file
  - configuration script, specifying options

- Specify the backup path, i.e., the directory in which the configuration is to be saved.
- Indicate how the file name of the backup file is to be structured. Placeholders can be used for device information (IP address, hardware type, etc.) and time information. Please refer to the online help for the ‘Backup filename’ parameter for further information on configuring this parameter.

5 Managing Device Configurations with the AutoConfiguration Adapter

If you are using a AutoConfiguration Adapter (ACA), WEBconfig allows you to save the device configurations on this external storage medium. In the case of a reboot, you have the option of transferring the configuration settings in the ACA manually or automatically to unconfigured devices.
A ACA has the following advantages:

- In case you need to replace the device, you can assign the previous configuration to the replacement device in order to get it quickly ready for operation.
- When you are setting up multiple devices of the same type, the ACA simplifies the first configuration.

You connect the ACA to the serial interface of the OpenBAT device.

5.1 Manually Transferring Device Settings to the ACA

Before you can transfer a configuration from the ACA to a device, you need to save that configuration to the ACA. A configuration can be saved in either of two different file types:

- Configuration: A full configuration file in the format *.lcf is transferred to the ACA. This configuration contains settings for a specific device — e.g. the name or site of the device.
- Script: A script file in the format *.lcs is transferred to the ACA. A script can contain, in contrast to a configuration file, certain parts of a configuration. Information which depends on the device — e.g. name or site of the device — can be managed through variables.

To transfer device settings to a ACA, follow these steps:

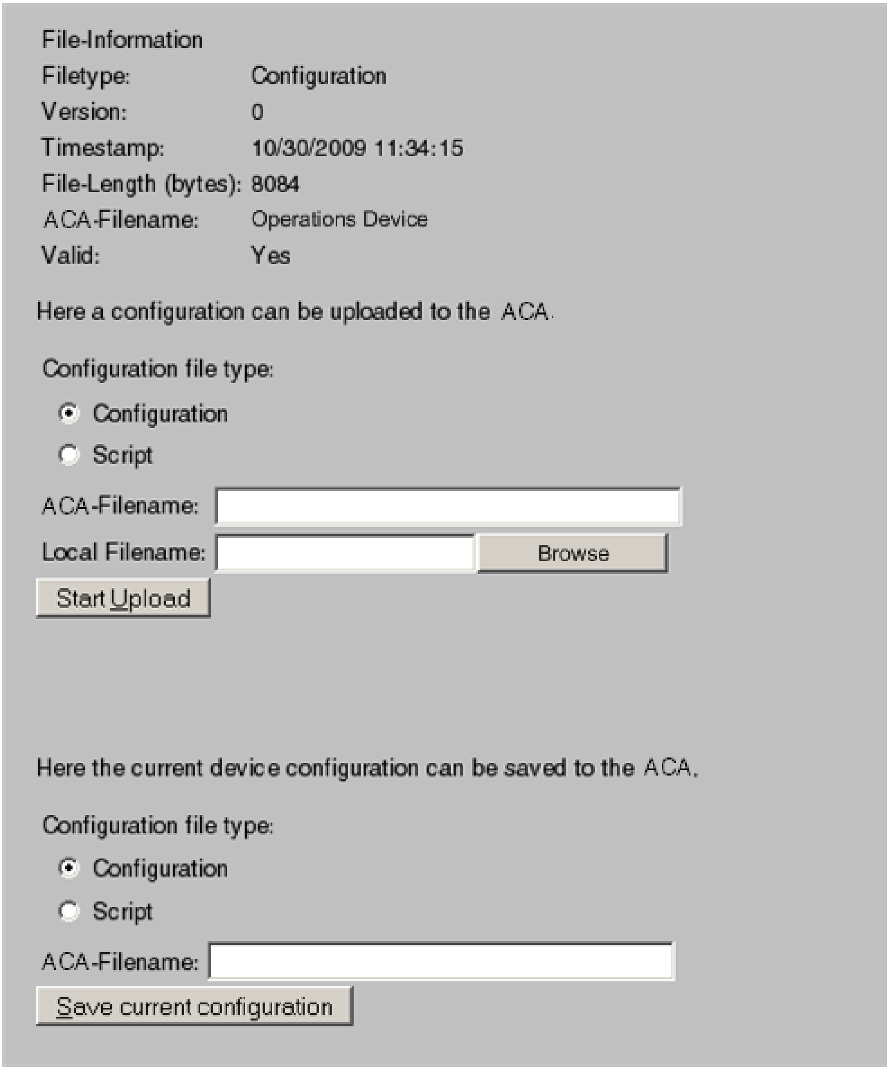
☐ Connect the ACA to the serial interface of the OpenBAT device.

☐ Use WEBconfig to login to the embedded web pages of the source device.

☐ Call up the following command in WEBconfig:

```
File Management : Upload file to ACA
```

The following dialog opens:



File-Information

Filetype:	Configuration
Version:	0
Timestamp:	10/30/2009 11:34:15
File-Length (bytes):	8084
ACA-Filename:	Operations Device
Valid:	Yes

Here a configuration can be uploaded to the ACA.

Configuration file type:

● Configuration

○ Script

ACA-Filename:

Local Filename:

Here the current device configuration can be saved to the ACA.

Configuration file type:

● Configuration

○ Script

ACA-Filename:

- ▶ If you want to transfer a configuration file or a script from an external storage medium to the ACA:
  - □ Select a file type: configuration or script

☐ Enter a meaningful ‘ACA Filename’.

☐ Click ‘Browse’, navigate to the path of the configuration file and select it.

☐ Click ‘Start Upload’ to copy the selected file to the ACA.

▶ If you want to transfer the current configuration of the device to the ACA:

☐ Select a file type: configuration or script

☐ Enter a meaningful ‘ACA Filename’.

☐ Click ‘Browse’, navigate to the path of the configuration file and select it.

☐ Click ‘Save current configuration’ to copy the device’s present configuration settings to the ACA.

Note: During the reading process, the Power LED flashes yellow.

5.2 Automatically Uploading Settings from the ACA to the Device

This is how you automatically upload the configuration settings from the ACA to the OpenBAT device:

☐ Connect the ACA to the serial interface of the OpenBAT device.

☐ Depending on the configuration status of the device, execute one of the following steps:

  ☐ If the device has never been configured before, switch on the device.

  ☐ If the device has already been configured, switch on the device and set up the factory settings.

During a reboot, an unconfigured device detects the connected ACA and automatically takes over the configuration settings from the ACA. During the reading process, the Power LED flashes yellow.

Note: If an incorrect or unsuitable configuration is stored on the ACA (e.g. if the configuration on the ACA belongs to another device type or another firmware), it is no longer possible to access the device via a LAN or WLAN interface. In this case, you transfer the correct configuration to the device via the serial interface.

5.3 Manually Uploading Settings from the ACA to the Device

To manually transfer device settings from a ACA to a device, follow these steps:

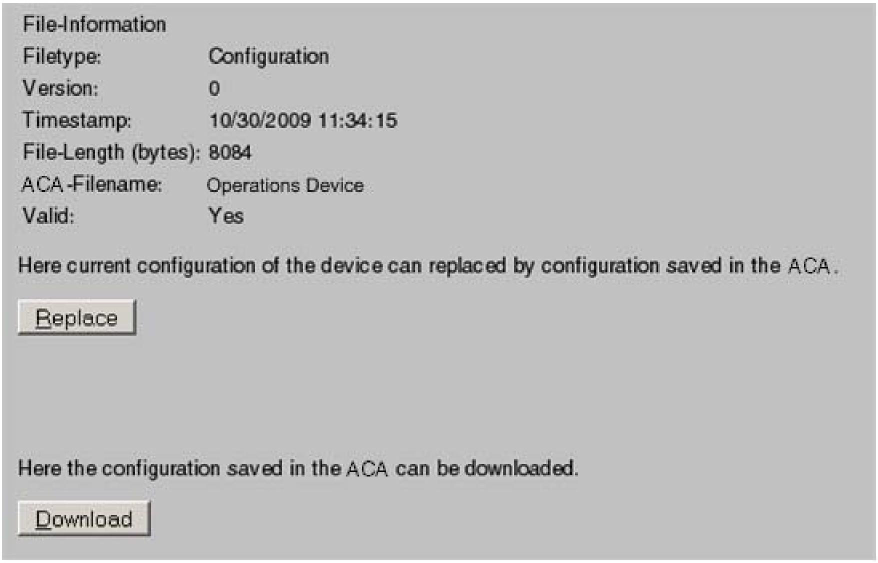
□ Connect the ACA to the serial interface of the target OpenBAT device.

□ Use WEBconfig to login to the embedded web pages of the target device.

□ Call up the following command in WEBconfig:

🟦 `File Management : Download a file from ACA`

The following dialog opens:



File-Information

Filetype: Configuration

Version: 0

Timestamp: 10/30/2009 11:34:15

File-Length (bytes): 8084

ACA-Filename: Operations Device

Valid: Yes

Here current configuration of the device can replaced by configuration saved in the ACA.

Here the configuration saved in the ACA can be downloaded.

☐ Indicate if the current configuration from ACA should be transferred to the device or should be saved to an external storage medium:

  ☐ If the current configuration of the device should be replaced with the configuration in the ACA, click ‘Replace’.

  ☐ If a configuration or script from the ACA should be transferred to an external storage medium choose ‘Download’.

Note: After the transmission of the configuration from ACA to the device, the new configuration is immediately active. In case of an incorrect or inappropriate configuration on the ACA, the device may no longer be accessible over a LAN or WLAN interface. In this case, either:

– use the serial interface to apply an appropriate configuration,

– or perform a system reset and restart the configuration process.

6 Rollout Wizard

In complex scenarios with multiple OpenBAT devices at various locations, it is possible that there is no qualified technician at the location where the OpenBAT device is being used who can perform the installation and the configuration. You can already carry out a significant part of the configuration in advance. Then the employees on site only have to set a few location-specific parameters.

The rollout wizard enables the on-site employees to perform these final steps with a browser. After the rollout wizard has been run, the device is either ready for operation or it can automatically get the missing configuration data from a central data storage. You will find the parameters for the configuration in WEBconfig at the following path:

■ `HiLCOS Menu Tree : Setup : HTTP : Rollout Wizard`

6.1 Settings for the Rollout Wizard

▶ Operating:
Switches the rollout wizard on or off. After you have switched it on, you will find the wizard on the start page of WEBconfig.
- Possible values: Yes / No
- Default: No

▶ Title:
Name for the rollout wizard that is displayed on the start page of WEBconfig.
- Possible values: Maximum 64 alphanumeric characters
- Default: Rollout

▶ Display Connection Status for:
This setting allows you to display the connection status of a DSL connection.

6.2 Variables

A maximum of ten variables can be defined with Index, Indent, Title, Type, Min. Value, Max. Value and Default Value.

- Index:
  Index for the variable. The Rollout Wizard displays the variables in ascending order.
  - Possible values: 1 to 4294967295
  - Default: 0
- Indent:
  Unique identifier of variables that are referenced during the execution of actions. Identifiers are not required for fields that are not used by users to enter their data (e.g. label).
  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank
- Title:
  Name of the variable as displayed by the Rollout Wizard in WEBconfig.
  - Possible values: Maximum 64 alphanumerical characters
  - Default: blank
- Type:
  Name of the variable as displayed by the Rollout Wizard in WEBconfig. Possible values include the following:
  - Label: Text that is displayed to provide explanations of the other variables. Min. Value and Max. Value are not significant for these entries.
  - Integer: Allows the entry of a positive integer number between 0 and 4294967295. By entering the Min. Value and Max. Value, the range of entries can be limited. Also, a default value can be defined. This default value must be between the Min. and Max. Values.
  - String: Enables text to be entered. By entering the Min. Value and Max. Value, the length of the string can be limited. Also, a default value can be defined. If this default text is longer than the maximum length, it will be truncated.
  - Password: displayed while being entered. Repeat entering the password. The Rollout Wizard will execute no actions if the passwords are different.
  - Checkmark: Simple option that can be switched on or off. Checkmarks are activated as standard if the default value is other than empty and

  the action executed accordingly.
  - Default: Label

▶ Min. Value:
Minimum value for the current variable (if type = integer) or minimum number of characters (if type = String or Password).
- Possible values: 0 to 4294967295
- Default: 0

▶ Max. Value:
Maximum value for the current variable (if type = integer) or maximum number of characters (if type = String or Password).
- Possible values: 0 to 4294967295
- Default: 0

▶ Default value:
Default value of the current variable.
- Possible values: Maximum 64 alphanumerical characters
- Default: blank

6.3 Actions Executed by the Rollout Wizard

A maximum of 19 definitions (with index and action) can be executed by the Rollout Wizard once the user data has been entered.

- Index:
  Index for the action. The Rollout Wizard executes the actions in ascending order.
  – Possible values: 1 and 4294967295
  – Default: 0

- Action:
  Action to be executed by the Rollout Wizard once the user data has been entered.
  – Possible values: Similar to Cron commands, actions are entered with the syntax “[Protocol:]Argument”. If no protocol is entered, 'exec.' is applied.
  – exec: Executes any command in the same way it is used in Telnet to configure a OpenBAT. The following example sets the name of the device to “MyWLANDevice”:
  `exec: set /setup/name MyWLANDevice`
  – mailto: Enables an e-mail to be sent upon entry of the address, subject and body text, for example:
  `mailto:admin@mywlandevice.de?subject=Rollout?body=WLANDevice setup completed`
  To make use of the mail function, set up an simple mail transfer protocol (SMTP) account in the device.
  – https and http: Enables a Web site to be accessed, for example to carry out an action:
  (`<https:|http:>//[user[:pass]@]hostname[:port]/...`)
  – Variables in the actions: When actions are executed, the values as defined with the Rollout Wizard can be referenced. The variable's identifier is used for the action with a leading percent character. Enclose the identifier in curly brackets if other alphanumeric characters are included in the action. The following example sets the name of the device to the format “Site (branch)”, if the location of the device is being queried as a variable with the identifier “Location”:

`exec: set /setup/name %{Location}(branch).`
For variables of the type Integer or String, the value as entered by the user is used. In the case of variables of the type Checkmark, “1” (switched on) or “0” (switched off) is used. If the expression for the action contains spaces, enclose the expression in quotation marks.

– Default: blank

▶ Description:
Description of the action.

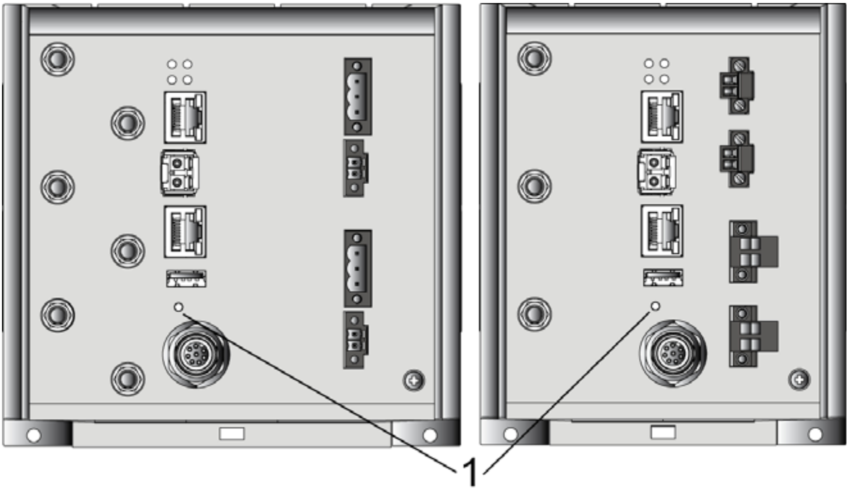
6.4 Actions for Managing the Rollout Wizard

- Renumber variables / Renumber actions:
  As explained above, variables and actions are displayed or processed in the order of their index. Occasionally, variables or actions with neighboring index numbers require a new entry to be entered between them. The indices can then be automatically renumbered with a specified interval between them.

  When being executed, the arguments can be defined with the start valueand an increment. This action renumbers the entries starting with the start value and continuing with the increment as chosen. If the start value and increment are not defined, both are set automatically to 10. If no arguments are entered, the action renumbers the indices with 10, 20, 30, etc.

7 Resetting and Re-Starting the Device

The OpenBAT device has a reset button.



1: Reset button

7.1 Default Reset Behavior

The reset button offers two basic functions, which are activated by holding down the Reset button for different lengths of time:

- Restart: Restarts the device and loads the current configuration settings. To restart the device, press the reset button only briefly.
- Reset: Resets the device to the factory settings. Press the reset button for around 5 seconds, or until the LEDs light up red. When you release the button, the device activates the factory settings (state on delivery).

Note: Create and store a copy of the current device configuration before pressing the reset button. After the button is pressed and held down for about 5 seconds, the existing configuration settings will be discarded and replaced by the factory default settings.

⚠ WARNING

LOSS OF CONFIGURATION DATA

Never press the reset button when the access point is operating.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Note: Save the current configuration of the device before the reset. After a hard reset, the device re-starts in the non-configured state, and all settings are lost.

7.2 Disabling the Reset Button

For some applications, you want to deactivate the reset button or limit the effect of pressing the reset button. In WEBconfig you change the behavior of the reset button on the following path:

```
HiLCOS menu tree : Setup : Config : Reset-button
```

The following settings are available for the reset button:

- Ignore:
  Deactivates the reset button on the device.
- Only boot:
  When you press the reset button, you restart the device while keeping the current device configuration.
- Reset or boot:
  Pressing the reset button briefly causes a restart. Pressing it for 5 seconds or longer causes a restart and resets the configuration to the factory settings. This is the default setting.

Note:

- With the “Ignore” or “Only boot” setting you prevent the device configuration from being reset to the factory settings with the reset button. If you lose the device password, you have no option to access the device via LAN or WLAN in order to reset the device configuration. In this case, you can use the serial communication interface to load the new firmware version to the device. You thus reset the device to the factory settings.
- During a reset, the WLAN encryption settings defined in the device are also lost, being reset to the standard WPA key. The wireless configuration of a device with a WLAN interface is only possible after the reset if the standard WAP key is programmed in the WLAN card.

8 Updating Firmware

Always use the latest firmware version for your OpenBAT device. Visit the Hirschmann website regularly (www.hirschmann.de) to check the availability of firmware updates and download the latest firmware versions.

Note: Save all the versions of the device firmware in the same folder, which serves as your firmware archive.

The OpenBAT device allows you to update the firmware while also saving the previous firmware version on the device. If necessary, you can reinstall the previous firmware version. If the new firmware has not been installed successfully, the device automatically activates the previous version.

This chapter shows you how to install the new firmware successfully using the following tools and procedures:

- LANconfig
- WEBconfig (embedded web pages)
- Terminal program (e.g. command line interface)
- tftp

8.1 How FirmSafe Works

FirmSafe overwrites the existing firmware and also saves it in the device. Thus your device is protected against the consequences of a power loss or connection interruption during the firmware installation.

Of the two firmware versions stored in the device, only one is ever active. When a new firmware is being loaded, the existing firmware version is kept as a backup copy. You can decide yourself which firmware is to be activated after the upload:

- “Immediately”: Loads the new firmware and activates it immediately. The following situations can then arise:
  - The new firmware is loaded successfully and then works as desired.
  - After the new firmware is loaded, the device cannot be addressed any more. If an error occurs during the upload, the device automatically reactivates the existing firmware, and thus restarts.
- “Login”: Uploads the firmware and starts the system immediately.
  - In contrast to the “Immediately” option, the device waits for the login for the duration of the Firmsafe timeout. You set the timeout value as follows:
– with WEBconfig under:
`HiLCOS menu tree : Firmware :Firmsafe timeout`
– for Telnet with “Firmware/Firmsafe timeout”
If the login attempt is successful, the device activates the new firmware.
  - If the device cannot be addressed any more, or if a login is not possible for other reasons, the device automatically reactivates the existing firmware, and thus restarts.
- “Manually”: With this option, you yourself specify a time period within which you want to test the new firmware. The device starts with the new firmware and waits for the specified time period. You then activate the new firmware manually:
– with LANconfig under `Device : Firmware management :Release`

`firmware running in test`,
– with Telnet under “Firmware/Firmsafe table” with the command “set # active”. Here # is the position of the firmware in the Firmsafe table.
– in WEBconfig you will find the Firmsafe table under
`HiLCOS menu tree : Firmware`.

You select the method for the Firmware upload as follows:

- under WEBconfig:`HiLCOS menu tree : Firmware : Mode-Firmsafe`
- under Telnet: “Firmware/Firmsafe timeout”
- under LANconfig you select the method when selecting the new firmware file

Note: It is then only possible to load a second firmware version if the device has enough memory space for two firmware versions. Current firmware versions may require more than half of the available memory space.

8.2 How to Load New Firmware

There are four methods to perform a firmware upload:

- LANconfig
- WEBconfig
- Terminal program
- tftp

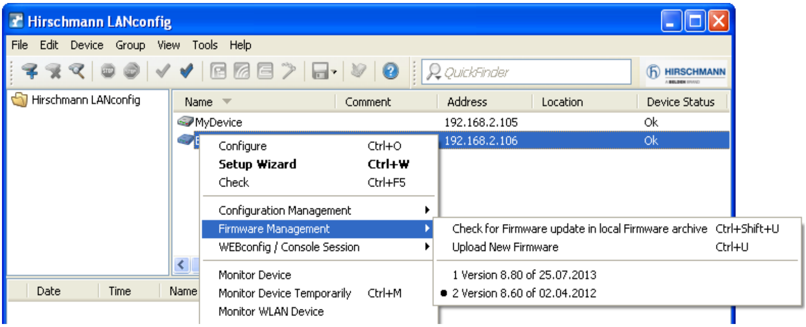
Before uploading, save the configuration and a version of the current firmware.

If the newly installed release contains parameters which are not present in the device's current firmware, the device will add the missing values using the default settings.

8.2.1 LANconfig

To upload new firmware using LANconfig, follow these steps:

□ Highlight the desired device in the selection list, then select: `Device : Firmware Management : Upload New Firmware`.


Hirschmann LANconfig
File Edit Device Group View Tools Help
QuickFinder
HIRSCHMANN
Hirschmann LANconfig
Name Comment Address Location Device Status
MyDevice 192.168.2.105 Ok
192.168.2.106 Ok
Configure Ctrl+O
Setup Wizard Ctrl+W
Check Ctrl+F5
Configuration Management
Firmware Management
WEBconfig / Console Session
Monitor Device
Monitor Device Temporarily Ctrl+M
Monitor WLAN Device
Check for Firmware update in local Firmware archive Ctrl+Shift+U
Upload New Firmware Ctrl+U
1 Version 8.80 of 25.07.2013
● 2 Version 8.60 of 02.04.2012
Date Time Name

A file selection dialog opens.

□ In the file selection dialog, select the new firmware file.

▶ Optionally, you can select ‘After upload, start the new firmware in test mode’, and specify a time, in minutes, for the duration of test mode.

□ Click `Open` to apply the selected firmware.

8.2.2 WEBconfig

Start WEBconfig in your web browser and follow the path starting at:

🟦 `Perform a Firmware Upload`

In the next window you can browse the folder system to find the firmware file. Click the following command to begin the installation:

🟦 `Start Upload`

8.2.3 Terminal Program

Examples of terminal programs include Telix or Hyperterminal in Windows. When using a terminal program, use the “set mode firmsafe” command in the “Firmware” menu to initially select the mode in which you want to load the new firmware (immediately, on login or manually). If desired, you can also set the duration of the firmware test using “set timeout firmsafe”.

Select the “do firmware upload” command to prepare the router to receive the upload, then start the upload procedure from your terminal program:

- If you are using Telix, click the `Upload` button. Specify “XModem” as the transfer protocol and select the desired file for the upload.
- If you are using Hyperterminal, click `Transfer : Send File`. Select the file, specify “XModem” as the protocol and start the transfer with `OK`.

Note: To use a terminal program for the firmware upload, you require a serial configuration interface.

8.2.4 TFTP

You can use tftp to install the new firmware on the OpenBAT device. You use the “writeflash” command for this. Example: To transfer a new firmware to a OpenBAT device with the IP address 10.0.0.1, enter the following command in Windows 2000 or Windows NT:

```
tftp -i 10.0.0.1 put Lc_16xxu.282 writeflash
```

8.2.5 Loading the Firmware via the Serial Interface with a Configuration Reset

The serial interface can also be used to load firmware into the device. Entering the serial number instead of the configuration password results in the device configuration being reset to its factory settings. This lets you re-open the device if the configuration password is lost and the reset button has been set to 'Ignore' or 'Boot only'.

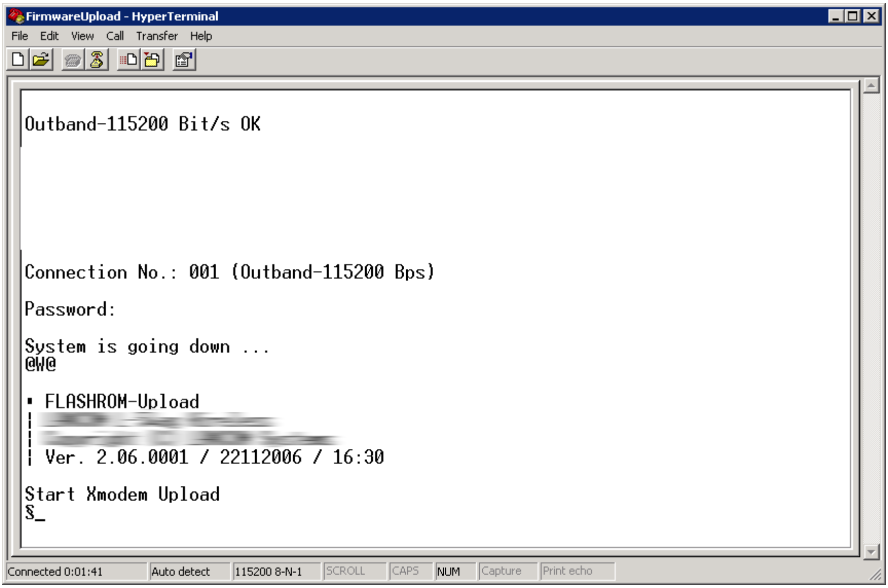
☐ Use the serial configuration cable to connect the device to a computer.

☐ Start a terminal program such as Hyperterminal.

☐ Open a connection with the settings 115200 bps, 8n1, hardware handshake (RTS/CTS).

☐ In the terminal program's welcome screen, press the Return key until the request to enter the password appears.

☐ Enter the serial number that is displayed under the firmware version and press Return again.



```
Outband-115200 Bit/s OK




Connection No.: 001 (Outband-115200 Bps)

Password:

System is going down ...
@W@

▪ FLASHROM-Upload
| [redacted]
| Ver. 2.06.0001 / 22112006 / 16:30

Start Xmodem Upload
§_
```

□ The device now expects the firmware upload. If you are using Hyperterminal, click `Transfer : Send File` to start the upload. Select “XModem” as the transfer protocol.

Note: Uploading the firmware in this way overwrites the configuration with the default factory settings. Consequently, this option should only be used if the configuration password is no longer available.

8.3 Searching for New Firmware

After you have obtained new firmware for your devices, you can simplify the firmware update for the OpenBAT devices by saving the new firmware files in a central firmware archive. Over time, this firmware archive can accumulate many firmware versions. Either search this archive manually for new firmware versions or have the search executed automatically every time LANconfig is started.

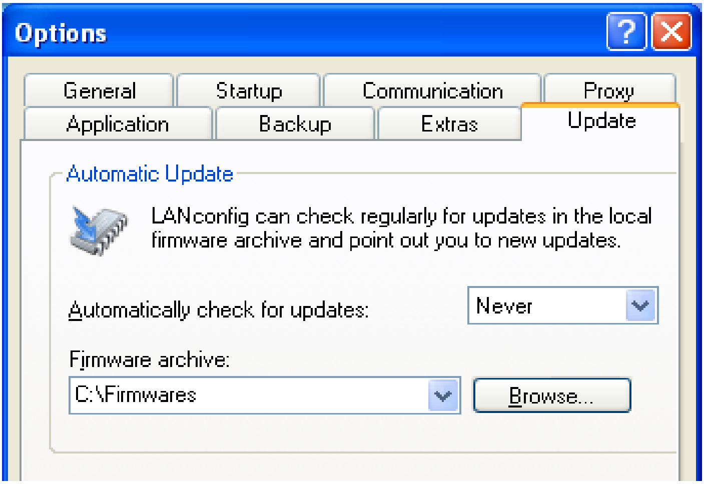
8.3.1 Automatic Search for Firmware Updates

If your firmware archive contains many version files, you may want to let LANconfig identify the specific files that apply to your devices. You can configure LANconfig to automatically perform the following tasks on startup:

- scan the central firmware archive to identify its contents, then
- identify those networked devices to which a firmware update applies

To do this, take the following steps:

□ In LANconfig, open the `Tools : Options : Update` dialog.



LANconfig can check regularly for updates in the local firmware archive and point out you to new updates.

Automatically check for updates: Never

Firmware archive: C:\Firmwares

□ Select a search interval from the dropdown list.

□ To identify the ‘Firmware archive’, click ‘Browse...’ then navigate to and select the central firmware archive.

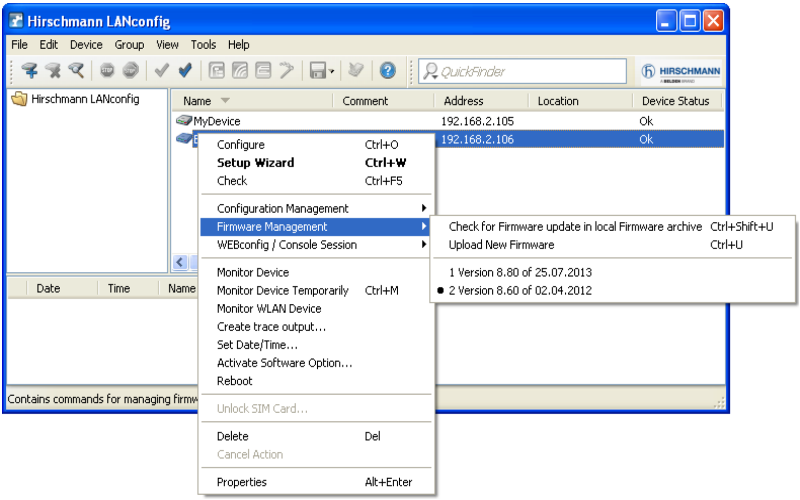
Note: The central firmware archive is where you should keep all device firmware files.

Each time LANconfig starts up, it automatically identifies the devices for which firmware updates are available in the specified firmware archive.

8.3.2 Manually Search for Firmware Updates

You can also manually manage the firmware update process. To do so, follow these steps:

☐ In LANconfig, right-click on one or more devices in the list. Then in the popup menu, select:
`Firmware Management : Check for firmware update in local Firmware archive`



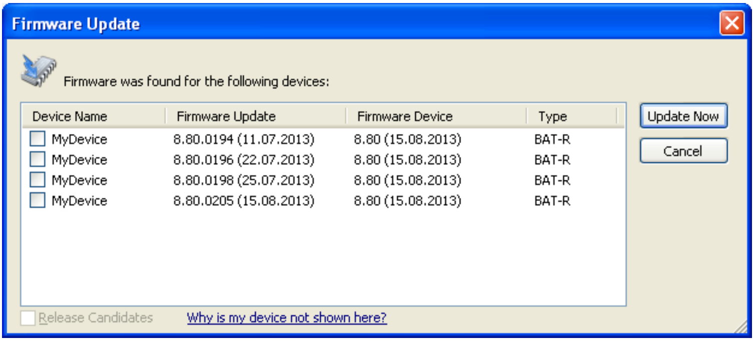
Name	Comment	Address	Location	Device Status
MyDevice		192.168.2.105		Ok
		192.168.2.106		Ok

Hirschmann LANconfig
File Edit Device Group View Tools Help
QuickFinder
HIRSCHMANN
Hirschmann LANconfig
Date Time Name
Contains commands for managing firmw
Configure Ctrl+O
Setup Wizard Ctrl+W
Check Ctrl+F5
Configuration Management
Firmware Management
WEBconfig / Console Session
Monitor Device
Monitor Device Temporarily Ctrl+M
Monitor WLAN Device
Create trace output...
Set Date/Time...
Activate Software Option...
Reboot
Unlock SIM Card...
Delete Del
Cancel Action
Properties Alt+Enter
Check for Firmware update in local Firmware archive Ctrl+Shift+U
Upload New Firmware Ctrl+U
1 Version 8.80 of 25.07.2013
● 2 Version 8.60 of 02.04.2012

LANconfig checks the ‘Firmware archive’ folder to see if it contains firmware updates for any of the selected devices.

8.3.3 Viewing All Device Firmware Versions

If your search in the archive does not reveal a new firmware version, you can view a full list of all of the firmware files and, for example, switch back to an older version. LANconfig displays all versions found for the selected devices, including the version currently active in each device. For each device, you can select one firmware version, which will then be uploaded to the device.



Firmware was found for the following devices:

Device Name	Firmware Update	Firmware Device	Type
□ MyDevice	8.80.0194 (11.07.2013)	8.80 (15.08.2013)	BAT-R
□ MyDevice	8.80.0196 (22.07.2013)	8.80 (15.08.2013)	BAT-R
□ MyDevice	8.80.0198 (25.07.2013)	8.80 (15.08.2013)	BAT-R
□ MyDevice	8.80.0205 (15.08.2013)	8.80 (15.08.2013)	BAT-R

□ Release Candidates

9 Load Files to the Device via tftp, http(s) or scp

Certain functions cannot be run, or run satisfactorily, via Telnet. These functions include those where entire files are transferred, such as the upload of firmware, and saving or restoring configuration data. Use tftp or http(s) in these cases.

9.1 TFTP

In Windows operating systems, tftp enables the transfer of files to/from other devices over the network. The syntax of the tftp call is dependent on the operating system. The syntax under Windows:

```
tftp -i <IP address Host> [get|put]
source [destination]
```

Note: The ASCII format is pre-configured on many tftp clients. Binary transmission therefore usually needs to be selected explicitly for the transfer of binary data (such as firmware). Parameter '-i' is used in this example for Windows.

If the device is password-protected, include the user name and password in the tftp command. The file name is either made up of the master password and the command to be executed (for supervisors), or of the combined user name and password separated by a colon (for local administrators) and with the command as a suffix. Therefore, a command sent via tftp looks like this:

- <Master password><Command>
- <User name>:<Password>@<Command>

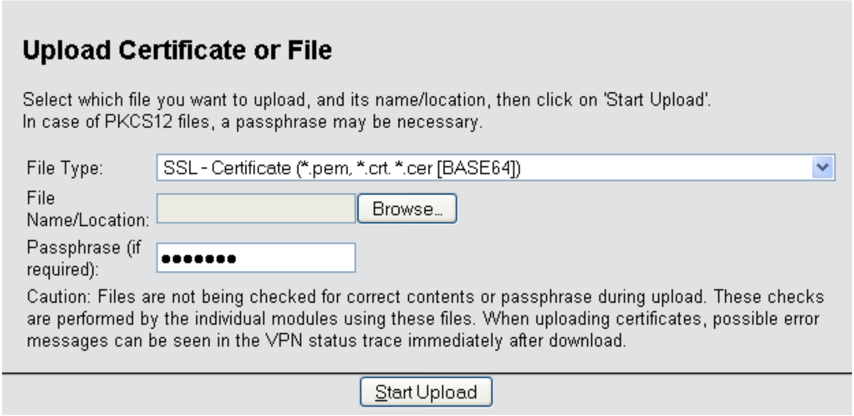
The rights to use tftp can be restricted for administrators.

9.2 Loading Firmware, Device Configuration or Script via http(s)

OpenBAT devices can also use http and https to download firmware, device configurations or scripts for automatic processes (e.g. to obtain files from the Internet themselves). In practice, it is easier to provide a central https server with a unique Internet address (URL) than a comparable tftp server. You can modify an existing Web server for this function.

An optional certificate for the https server can be uploaded by WEBconfig to the device as the SSL root CA certificate at the following location:

■ `File management : Upload Certificate or File`



Upload Certificate or File

Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.

File Type:	SSL - Certificate (*.pem, *.crt, *.cer [BASE64])
File Name/Location:	
Passphrase (if required):	●●●●●●●●

Caution: Files are not being checked for correct contents or passphrase during upload. These checks are performed by the individual modules using these files. When uploading certificates, possible error messages can be seen in the VPN status trace immediately after download.

9.3 Loading Firmware, Device Configuration or Script via http(s) or tftp

In addition to the option to load firmware or a configuration file into a device using LANconfig or WEBconfig, Telnet and SSH can also be used to directly upload the relevant files from an HTTP(S) or tftp server. This process can simplify device administration in larger installations with regular firmware updates and/or configuration changes. HTTP(S) and tftp can also be used to load scripts (e.g. with partial configurations) into devices.

The firmware and configuration files or scripts are stored on an HTTP(S) or tftp server. A tftp server is identical to an ftp server in terms of functionality, but it uses a different protocol for data transmission. When using an https server, a certificate used to check the identity of the server can be stored on the device. The files can be retrieved from this server with the following commands:

- LoadConfig
- LoadFirmware
- LoadScript

The server, the directory and the file can be specified in two ways:

- By using the tftp protocol with parameters -s and -f:
  - `-s <Server IP address or server name>`
  - `-f <File path and file name>`
- By using tftp or HTTP(S), the command can be specified in the usual URL notation (either tftp or HTTP(S) is entered as the protocol):
  - `Command protocol://server/directory/file name`

    When accessing a password-protected area on an HTTP(S) server, the user name and password are entered accordingly:
  - `Command protocol://user name:password@server/directory/file name`

When using https, a certificate can be specified with which the identity of the server is checked:

– `-c <Certificate name>`

The following variables are permitted in the file name (including path):

- %m - LAN MAC address (hexadecimal, lowercase, no separators)
- %s - Serial number
- %n - Device name
- %l - Location (from the configuration file)
- %d - Device type

9.3.1 Examples

With the following command you load a firmware file with the name “LC-1811-5.00.0019.upx” from directory “HiLCOS/500” from the server with the IP address “192.168.2.200” to the device:

```
LoadFirmware -s 192.168.2.200 -f HiLCOS/500/LC-1811-5.00.0019.upx
```

In a Telnet session, with the following command you load a script that matches the MAC address from the server with the IP address “192.168.2.200” to the device:

```
LoadScript -s 192.168.2.200 -f %m.lcs
```

In a Telnet session, with the following command you load the firmware file “LC-1811-5.00.0019.upx” from the “download” directory from the https server with the IP address “www.myserver.com” to the device. The identity check of the server is performed with the certificate “sslroot.crt”:

```
LoadFirmware -c sslroot.crt https://www.myserver.com/download/LC-1811-5.00.0019.upx
```

If you do not enter the parameters `-s` and/or `-f`, the device uses the standard values that are set up on the path `/setup/config/TFTP-Client`:

- `Config address`
- `Config file name`
- `Firmware address`
- `Firmware file name`

It makes sense to use these standard values if the current configurations and firmware versions are always saved under the same name at the same location. In this case, you use the simple commands `LoadConfig` and `LoadFirmware` to load the corresponding valid file.

9.4 File Transfer via SCP

SCP (Secure Copy) is a protocol for the secure transfer of data between two computers in a network. Administrators often use SCP to exchange data between servers or between servers and workstations. With a suitable tool (e.g. the Putty add-on pscp.exe on Windows operating systems) you can also exchange data between your PC/notebook and a OpenBAT device.

Download pscp.exe from the Putty download page to perform file transfer from a Windows operating system.

Then open a command line window using the command `cmd`.

Change to the directory where you have saved the file pscp.exe and run the following command to transfer a file from your Windows computer to the device. Enter the options `-scp` and `-pw` followed by your password:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw
******* c:\path\myfile.ext <User>@<IP-
address>:target
```

Change the order of the source and destination, to transfer the file from the device to your computer:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw
******* <User>@<IP-address>:target
c:\path\myfile.ext
```

Enter the following command to save the configuration from the device to a file named `config.lcs` on your computer:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw
******* root@123.123.123.123:config c:\config.lcs
```

To upload a new firmware file from your computer to the device, enter the following command:

```
C:\PortableApps\PuTTYPortable>pscp.exe -scp -pw
******* c:\firmware.upx
root@123.123.123.123:firmware
```

The following table specifically shows which files you can read via SCP from the device and which ones you can write to it:

Table 1: Files for the SCP file transfer

Target	**Read**	**Write**	**Description**
Target	Read	Write	Description
ssl_cert	Yes	Yes	SSL – certificate (*.pem, *.crt. *.cer [BASE64])
ssl_privkey		Yes	SSL – private key (*.key [BASE64 unencrypted])
ssl_rootcert	Yes	Yes	SSL – root CA certificate (*.pem, *.crt. *.cer [BASE64])
ssl_pkcs12		Yes	SSL – container as PKCS#12 file (*.pfx, *.p12)
ssh_rsakey		Yes	SSL – RSA key (*.key [BASE64 unencrypted])
ssh_dsakey		Yes	SSL – DSA key (*.key [BASE64 unencrypted])
ssh_authkeys		Yes	SSH – accepted public key
vpn_rootcert	Yes	Yes	VPN – root CA certificate (*.pem, *.crt. *.cer [BASE64])
vpn_devcert	Yes	Yes	VPN – device certificate (*.pem, *.crt. *.cer [BASE64])
vpn_devprivkey		Yes	SSL – private device key (*.key [BASE64 unencrypted])
vpn_pkcs12		Yes	VPN – container (VPN1) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_2		Yes	VPN – container (VPN2) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_3		Yes	VPN – container (VPN3) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_4		Yes	VPN – container (VPN4) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_5		Yes	VPN – container (VPN5) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_6		Yes	VPN – container (VPN6) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_7		Yes	VPN – container (VPN7) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_8		Yes	VPN – container (VPN8) as PKCS#12 file (*.pfx, *.p12)
vpn_pkcs12_9		Yes	VPN – container (VPN9) as PKCS#12 file (*.pfx, *.p12)
vpn_add_cas		Yes	VPN - add additional CA certificates (*.pfx, *.p12, *.pem, *.crt. *.cer [BASE64])
eaptls_rootcert	Yes	Yes	EAP/TLS – root CA certificate (*.pem, *.crt. *.cer [BASE64])
eaptls_devcert	Yes	Yes	EAP/TLS – device certificate (*.pem, *.crt. *.cer [BASE64])
eaptls_privkey		Yes	EAP/TLS – private device key (*.key [BASE64 unencrypted])
eaptls_pkcs12		Yes	EAP/TLS – container as PKCS#12 file (*.pfx, *.p12)
radsec_rootcert	Yes	Yes	RADSEC – root CA certificate (*.pem, *.crt. *.cer [BASE64])
radsec_devcert	Yes	Yes	RADSEC – device certificate (*.pem, *.crt. *.cer [BASE64])
radsec_privkey		Yes	RADSEC – private device key (*.key [BASE64 unencrypted])
radsec_pkcs12		Yes	RADSEC – container as PKCS#12 file (*.pfx, *.p12)
radiuss_accnt_total	Yes	Yes	RADIUS server – summary accounting (*.csv)
scep_cert_list	Yes	Yes	SCEP-CA – certificate list
scep_cert_serial	Yes	Yes	SCEP-CA – serial number

Table 1: Files for the SCP file transfer

Target	Read	Write	Description
scep_ca_backup	Yes		Backup for SCEP-CA – PKCS12 container
scep_ra_backup	Yes		Backup for SCEP-CA – PKCS12 container
scep_ca_pkcs12		Yes	SCEP-CA – PKCS12 container
scep_ra_pkcs12		Yes	SCEP-CA – PKCS12 container
pbspot_template_welcome	Yes	Yes	Public Spot – welcome page (*.html, *.htm)
pbspot_template_login	Yes	Yes	Public Spot – login page (*.html, *.htm)
pbspot_template_error	Yes	Yes	Public Spot – error page (*.html, *.htm)
pbspot_template_start	Yes	Yes	Public Spot – home page (*.html, *.htm)
pbspot_template_status	Yes	Yes	Public Spot – status page (*.html, *.htm)
pbspot_template_logoff	Yes	Yes	Public Spot – logoff page (*.html, *.htm)
pbspot_template_help	Yes	Yes	Public Spot – help page (*.html, *.htm)
pbspot_template_noproxy	Yes	Yes	Public Spot – no proxy page (*.html, *.htm)
pbspot_template_voucher	Yes	Yes	Public Spot – voucher page (*.html, *.htm)
pbspot_template_agb	Yes	Yes	Public Spot – GTC page (*.html, *.htm)
pbspot_formhdrimg	Yes	Yes	Public Spot – header image pages (*.gif, *.png, *.jpeg)
WLC_Script_1.lcs	Yes	Yes	CAPWAP – WLC_Script_1.lcs
WLC_Script_2.lcs	Yes	Yes	CAPWAP – WLC_Script_2.lcs
WLC_Script_3.lcs	Yes	Yes	CAPWAP – WLC_Script_3.lcs
default_pkcs12		Yes	
rollout_wizard		Yes	
rollout_template		Yes	
rollout_logo		Yes	
hip_cert_0		Yes	
issue	Yes	Yes	Text for display after command-line login (e.g. ASCII logos)
config	Yes	Yes	Device configuration
firmware		Yes	Firmware update

10 Scripting

In installations with multiple OpenBAT devices, you might want to execute specific configuration tasks automatically. The scripting functions in the OpenBAT device allow you to save entire sets of commands for configuring the devices in one file (a script) and to transfer them to one or more devices in a single step.

10.1 Applications

Scripting provides users with a powerful tool for centrally configuring the OpenBAT devices, with a wide range of potential applications:

- Reading out the device configuration in a form that is easy to read and save:
  The configuration files created by LANconfig are not intended to be processed directly with other tools. Only by printing the configuration file will you get an overview of the complete configuration. The scripting functions allow you to output the configuration as an ASCII text and then save it as a simple text file.

- Editing the configuration with a simple text editor:
  If offline configuration with LANconfig is not possible or is not desired, you have the option of using a text editor to edit a configuration file created by scripting, then load it to the device again.

- Editing parts of a configuration:
  Instead of a complete configuration, you can also read specific parts of the configuration from a device (e.g. only the firewall settings). Just like with complete configurations, parts of configurations can be edited and then transferred to one or more devices. This gives you the option of loading specific settings in a device to other models or devices with a different firmware version.

- Automated configuration updates:
  The centralized storage of configuration scripts in combination with scheduled commands (cron jobs) can be used to update important parts of the configuration (e.g. the encryption settings for a WLAN) automatically in multiple devices at the same time.

- Convenient rollout in larger installations:
  If multiple devices are installed at different locations, it is very easy to control the configuration centrally. Employees without administrator rights can then set up the devices using a single command.

- Saving the configuration in volatile memory only:
  Scripting commands allow you to save the changes to the configuration in RAM only. Saving it to non-volatile memory is then not allowed. As a result, the configuration is only available until the next system booting.
- Changing the configuration in the test mode:
  The same mechanism allows you to change the configuration very easily in the test mode. You use a script to trigger a time-delayed system boot, and until the boot is activated you can change and test the configuration of the device. The device automatically reboots after the time delay and is reset to its previous configuration.
  Like the FirmSafe function, this variant also provides you with a kind of “ConfSafe”. If you make changes to the configuration after a firmware update, sometimes the configuration may no longer be editable after a subsequent downgrade to the old firmware version. However, if you only change the configuration in test mode after the firmware upgrade, you can very easily restore the original firmware and configuration status of the devices by downgrading and then rebooting.

10.2 Scripting Function

With scripting you transfer a series of configuration commands collectively to a OpenBAT – just as you would enter the commands in the Telnet console of the device, for example. There are two variants for this collective transfer of configuration commands:

- You put the device in console mode by entering the “beginscript” command in the script mode. In this mode the program does not execute the transferred commands individually, but initially writes them to the intermediate memory of the OpenBAT. Only when you enter the “exit” command does the program execute these commands.
- Alternatively, you can write the configuration commands offline to a script file (text file) and then upload them to the device as a complete script.

The configuration commands executed using the script file initially effect only the configuration that is stored in the RAM of the device. The flash mode then determines whether the configuration is also changed in the flash memory.

- In Flash Yes mode (standard), the configuration commands are directly written to the flash memory of the device, and are thus boot resistant. Since the flash mode is always ON with the other methods of configuration (console without script, LANconfig or WEBconfig), the configuration changes are written first to the RAM memory and then immediately to the flash memory
- In Flash No mode the data is written only to RAM and is thus available only until the next boot.
  - During the boot process, the device reads the configuration data from the flash memory.
  - At any time, you can transfer the configuration from the RAM to the flash memory using the command “Flash Yes”. When actively operating, the OpenBAT devices use the information stored in the RAM configuration. The script commands stored in the intermediate memory are, like the configuration in flash memory, not relevant to the real-time operations of a OpenBAT device.

10.3 Generate Script Files

A script for a OpenBAT configuration is a conventional text file. This includes any necessary comments and all of the commands used to set the configuration, for example when using a Telnet console. There are two ways to generate a script file:

- The configuration, or a section of it, can be read out of a device, stored as a script file and then altered with a suitable text editor.
- The script can be generated entirely with a text editor.

10.3.1 Reading Out the Configuration via the Console

To read the configuration out of the console, follow these steps:

□ Log on to the console with write access rights.

□ Switch to the branch of the configuration tree that you wish to read out.

□ At the command prompt, execute the command readscript. Observe the optional command extensions (Scripting commands).

□ Using the Clipboard, copy and paste the required text section into a text editor and adapt the script to your requirements.

10.3.2 Reading the Configuration via TFTP from the CLI

The configuration commands can be read out directly from the command line interface (DOS command line interface) via tftp. Note that device passwords will be clearly visible as plain text while entering this command. Do the following:

□ Open a DOS screen.

□ Enter the following command at the prompt:

```
C:\>tftp IP address get “PASSWORDreadscript path”
script.lcs
```

□ “IP address” is the address of the device containing the configuration commands you wish to read out.

– PASSWORD is the appropriate password for the device.

– “Path” defines the branch of the configuration menu tree that is to be read out. If no path is entered then the entire configuration will be read out.

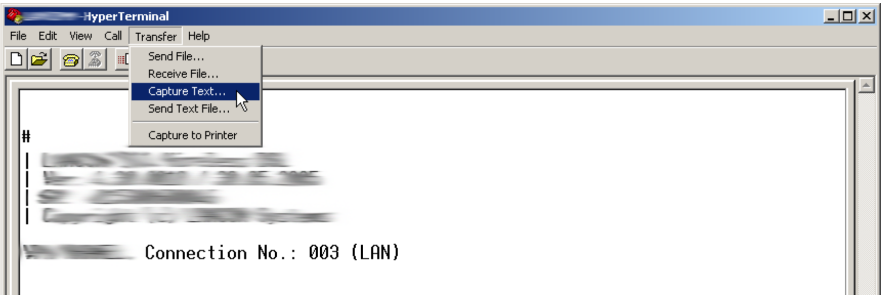
– `script.lcs` is the name of the script file in the current directory where the commands will be written.

10.3.3 Reading the Configuration with Hyperterminal

Terminal programs such as Hyperterminal provide the option of storing the text displayed by the console directly to a text file. This method is advantageous when dealing with larger configuration files, as it avoids the potentially confusing method of using the Clipboard. Follow these steps:

□ Set up a connection to the device with Hyperterminal.

□ Select the menu item `Transfer : Capture Text` and select the desired storage location and file name for the script.



```
#
Connection No.: 003 (LAN)
```

☐ At the command prompt, execute the command readscript. Observe the optional command extensions.

☐ After you have called up all required sections of the configuration, stop the recording with the following menu item:
`Transfer : Capture Text : Stop.`

The configuration commands are now available as a script file and can be altered as required.

10.3.4 Download Script from the Device

In installations with multiple OpenBAT devices, you might want to execute specific configuration tasks automatically. The scripting functions in the OpenBAT device allow you to save entire sets of commands for configuring the devices in one file (a script) and to transfer them to one or more devices in a single step.

In addition to manually creating a script and reading via the console, you can also use LANconfig to read script files from a device. To do this, right-click on the corresponding entry in the device list, and in the context menu select `Configuration Management : Save script to file`. Select the following options:

- Numeric section
  Enable this option if you do not want the configuration sections in the script to be displayed numerically (e.g. /2/2/5), rather than in clear text (/ setup/wlan/ppp).
- Default values
  Unless defined otherwise, the parameters saved in a script are always only those that deviate from the default values. Enable this option if you also want the default values to be entered in the script.
- Column names
  Unless defined otherwise, the fields in a table are initially entered as column names in the scripts, after which the respective values are inserted into the rows. Enable this option if you want every value in the table to be explicitly given the name of the column in which it is stored.
- Comments
  Enable this option if you want to include additional comments in the script file.
- Compact formatting
  Enable this option to suppress spaces and tabs.
- Download only selected sections
  Unless defined otherwise, the program always saves the entire device configuration in a script. By defining specific script sections, you can also save parts of configurations. In this field you enter the sections that you want transferred to the script (e.g. /setup/wlan).

10.4 Uploading Configuration Commands and Script Files

You have 2 different methods for loading the script commands to the intermediate memory of the OpenBAT device:

▶ You enter the commands manually at a console in script mode with the command “beginscript”. You thus write the commands directly from the console to the intermediate memory. When you have completed all the commands, enter the command “exit” to transfer them to the RAM.

▶ You save the desired command sequence in a text file. This text file is then transferred to the intermediate memory using the corresponding tool (LANconfig, terminal program, TFTP). If the file contains the required commands, the program automatically begins transferring the configuration to the RAM.

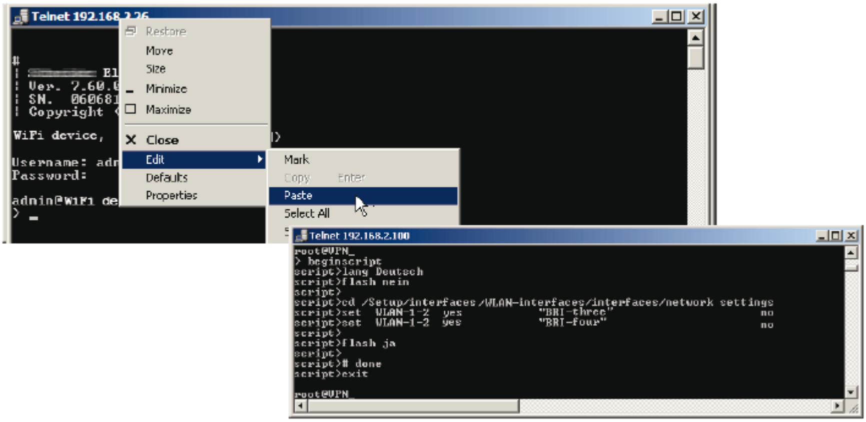
10.4.1 Entering Commands in a Console Session (Telnet, SSH)

In a console session, a script can be uploaded to the device via the Clipboard, as follows:

□ Open your script with any text editor and transfer the configuration commands to the Clipboard.

□ Log on to the console with Supervisor rights.

□ Start the script mode with the command `beginscript`.



```
#
| [redacted] El
| Ver. 7.60.0
| SN.  060681
| Copyright (

WiFi device,

Username: adm
Password:

admin@WiFi de
> _
```

```
root@VPN_
> beginscript
script>lang Deutsch
script>flash nein
script>
script>cd /Setup/interfaces/WLAN-interfaces/interfaces/network settings
script>set  WLAN-1-2  yes              "BRI-three"                   no
script>set  WLAN-1-2  yes              "BRI-four"                    no
script>
script>flash ja
script>
script># done
script>exit

root@VPN_
```

- □ Paste the commands from the Clipboard after the script prompt (`script>`). In Telnet, for example, right-click on the upper frame of the window.
- □ Entering the command `exit` executes the configuration commands.

  Note: If the command `exit` is already included in the pasted commands, execution of the configuration will be carried out automatically.

10.4.2 Tab Command when Scripting

When working with scripts, the `tab` command implements the columns in a table for the subsequent `set` command.

When you perform the configuration with a command line tool, you generally supplement the set command with the values for the columns of the table.

For example, you set the values for the performance settings of a WLAN interface as follows:

```
> cd /Setup/Interfaces/WLAN/Performance
> set ?Possible Entries for columns in Performance:
[1][Ifc]                : WLAN-1 (1)
[5][QoS]                : No (0), Yes (1)
[2][Tx-Bursting]        : 5 Chars from: 1234567890

> set WLAN-1 Yes *
```

In this example the Performance table has three columns:

- Ifc, the desired interface
- Enable or disable QoS
- The desired value for TX bursting

With the command `set WLAN-1 Yes *` you enable the QoS function for WLAN-1, and you leave the value for TX bursting unchanged with the asterisk (*).

Working with the `set` command in this way is adequate for tables with only a few columns. However, tables with many columns can pose a major challenge. For example, the table under `Setup:Interfaces:WLAN:Transmission` contains 22 entries:

```
> cd /Setup/Interfaces/WLAN/Transmission
> set ?Possible Entries for columns in Transmission:
[1][Ifc]                : WLAN-1 (1), WLAN-1-2 (16), WLAN-1-3 (17),
WLAN-1-4 (18), WLAN-1-5 (19), WLAN-1-6 (20), WLAN-1-7 (21), WLAN-1-8
(22)
[2][Packet-Size]        : 5 Chars from: 1234567890
[3][Min-Tx-Rate]       : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6),
6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M
(15)
[9][Max-Tx-Rate]       : Auto (0), 1M (1), 2M (2), 5.5M (4), 11M (6),
6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M
(15)
[4][Basic-Rate]       : 1M (1), 2M (2), 5.5M (4), 11M (6), 6M (8), 9M
(9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14), 54M (15)
[19][EAPOL-Rate]       : Like-Data (0), 1M (1), 2M (2), 5.5M (4), 11M
(6), 6M (8), 9M (9), 12M (10), 18M (11), 24M (12), 36M (13), 48M (14),
54M (15), HT-1-6.5M (28), HT-1-13M (29), HT-1-19.5M (30),HT-1-26M (31),
HT-1-39M (32), HT-1-52M (33), HT-1-58.5M (34), HT-1-65M (35), HT-2-13M
(36), HT-2-26M (37), HT-2-39M (38), HT-2-52M (39), HT-2-78M (40), HT-
2-104M (41), HT-2-117M (42), HT-2-130M (43)
[12][Hard-Retries]      : 3 Chars from: 1234567890
[11][Soft-Retries]      : 3 Chars from: 1234567890
[7][11b-Preamble]       : Auto (0), Long (1)
[16][Min-HT-MCS]       : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10
(3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15
(8)
[17][Max-HT-MCS]       : Auto (0), MCS-0/8 (1), MCS-1/9 (2), MCS-2/10
```

```
(3), MCS-3/11 (4), MCS-4/12 (5), MCS-5/13 (6), MCS-6/14 (7), MCS-7/15
(8)
[23][Use-STBC]          : No (0), Yes (1)
[24][Use-LDPC]         : No (0), Yes (1)[13][Short-Guard-Interval]  :
Auto (0), No (1)
[18][Min-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[14][Max-Spatial-Streams] : Auto (0), One (1), Two (2), Three (3)
[15][Send-Aggregates]   : No (0), Yes (1)
[22][Receive-Aggregates]: No (0), Yes (1)
[20][Max-Aggr.-Packet-Count]    : 2 Chars from: 1234567890
[6][RTS-Threshold]      : 5 Chars from: 1234567890
[10][Min-Frag-Len]      : 5 Chars from: 1234567890
[21][ProbeRsp-Retries]  : 3 Chars from: 1234567890
```

Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

```
set WLAN-1-3 * * * * * * * * * * * * No
```

Note: The asterisks for the values after the column for the short guard interval are unnecessary in this example, as the columns will be ignored when setting the new values.

As an alternative to this rather confusing and error-prone notation, you can use the `tab` command as the first step to determine which columns are changed with the subsequent `set` command:

```
tab Ifc Short-Guard-Interval
set WLAN-1-3 No
```

The `tab` command also makes it possible to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
tab Ifc Short-Guard-Interval Use-LDPC
set WLAN-1-3 No Yes
```

Note: The tables may only contain only a selection of the columns, depending on the hardware model. The `tab` command ignores columns which do not exist for that device. This gives you the option to develop shared scripts for different hardware models. The `tab` instructions in the scripts reference the maximum number of required columns. Depending on the model, the script only performs the `set` instructions for the existing columns.

You can also abbreviate the `tab` command with curly brackets. Use the following command to set the short guard interval in the transmission table for the WLAN-1-3 interface to No:

```
set WLAN-1-3 {short-guard} No
```

The curly brackets also enable you to change the order of the columns. The following example for the WLAN-1-3 interface sets the value for the short guard interval to `No` and the value for Use-LDPC to `Yes`, although the corresponding columns in the table are displayed in a different order:

```
set WLAN-1-3 {Short-Guard-Interval} No {Use-LDPC} Yes
```

10.4.3 Upload Script with TFTP Client

During a console session (e.g. via Telnet or SSH), tftp commands can beused to upload script files to the device directly from a tftp server, as follows:

□ Log on to the console with Supervisor rights.

□ Enter the following command at the prompt:

```
loadscript -s IP address -f script.lcs
```

□ IP address is the address of the TFCTP server where the script file is stored.

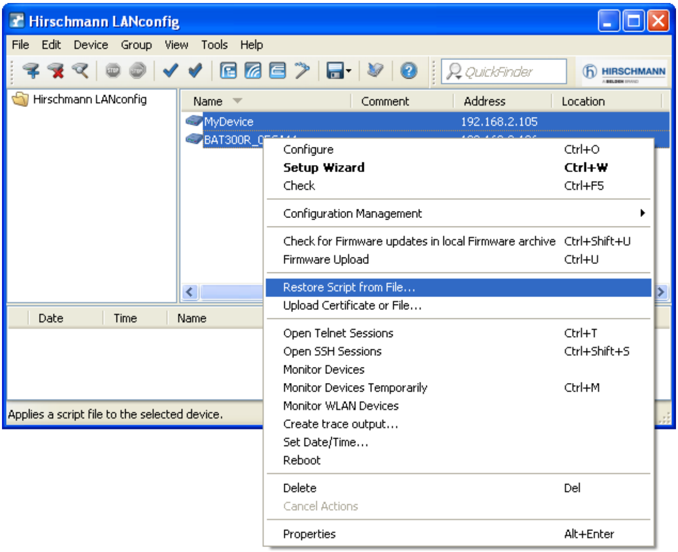
□ `script.lcs` is the name of the script file on the tftp server.

10.4.4 Upload Script with LANconfig

LANconfig has the option to upload a script either to a single device or to multiple devices simultaneously, as follows:

☐ Right-click on a device. Use the context menu to select the entry `Configuration Management : Restore Script from File`. If multiple devices are marked, the entry `Restore Script from File` appears directly in the context menu.

☐ In the following dialog, select the required script file (*.lcs) for upload.



Applies a script file to the selected device.

Note: The upload of the script starts automatically. Status and event messages are either displayed directly by LANconfig or can be viewed in a console session with the command `show script`.

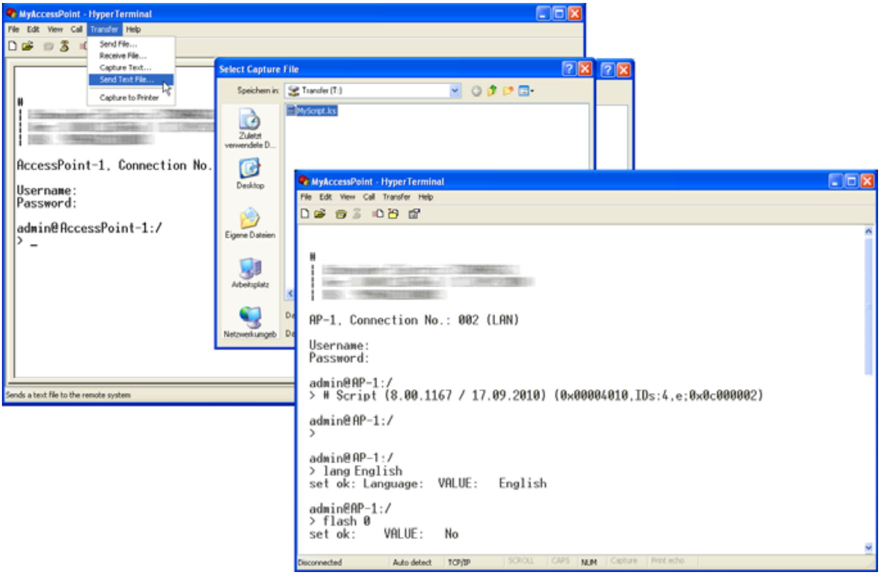
10.4.5 Upload Script with Hyperterminal

Another way to upload scripts to a OpenBAT device is to use terminal programs such as Hyperterminal, which is supplied with Windows.

☐ Set up a connection to the device with Hyperterminal.

☐ Select the menu item `Transfer : Send Text File`.

☐ Select a script file and start the transfer.



```
AccessPoint-1, Connection No.

Username:
Password:

admin@AccessPoint-1:/
> _
```

```
#
|
|
|

AP-1, Connection No.: 002 (LAN)

Username:
Password:

admin@AP-1:/
> # Script (8.00.1167 / 17.09.2010) (0x00004010,IDs:4,e:0x0c000002)

admin@AP-1:/
>

admin@AP-1:/
> lang English
set ok: Language:  VALUE:   English

admin@AP-1:/
> flash 0
set ok:     VALUE:   No
```

After successful completion of the transfer, the script starts automatically.

10.4.6 Multiple Parallel Script Sessions

The OpenBAT device can manage multiple parallel script sessions. Just as multiple console sessions can be run simultaneously on a single device, different scripts can also access the OpenBAT device in parallel. Parallel script sessions are useful in the following scenarios:

- Script 1 initiates a reboot of the device after a time delay of 30 minutes. Script 2 is active while the device is running and changes the configuration for test purposes. The flash mode remains deactivated for this. If the changes script 2 made to the configuration make the device unreachable, script 1 reboots the device after 30 minutes and thus rejects the changes to the configuration.
- When different scripts are being used for partial configurations, it is possible for multiple scripts to be started automatically at the same time, e.g. via cron jobs. You have the option of starting a task while other tasks are still running.

10.4.7 Scripting Commands

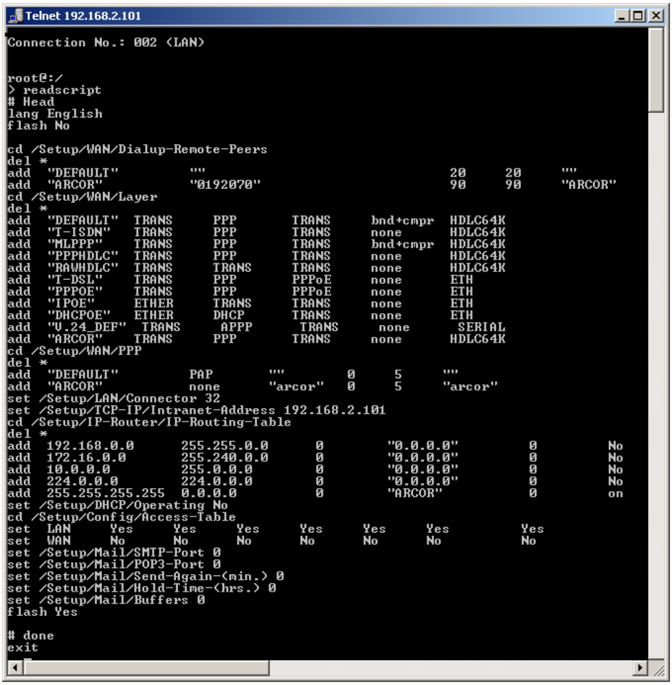
▶ `readscript`

In a console session, the “readscript” command creates a text output of all the commands and parameters required for the configuration of the OpenBAT device in its current state. In the simplest case, the OpenBAT only lists commands that are relevant to parameters that deviate from the factory settings.

Syntax: `readscript  [-n] [-d] [-c]  [-m]  [PATH]`

Note: Log on to the console with write access rights to execute this command.

For example, with a OpenBAT that is set up solely for Internet-by-call via ISDN, the readscript command will produce the following console output (assuming that there are no further restrictions):



```
Connection No.: 002 <LAN>


root@:/
> readscript
# Head
lang English
flash No

cd /Setup/WAN/Dialup-Remote-Peers
del *
add  "DEFAULT"         ""                               20     20     ""
add  "ARCOR"           "0192070"                        90     90     "ARCOR"
cd /Setup/WAN/Layer
del *
add  "DEFAULT"  TRANS     PPP       TRANS     bnd+cmpr  HDLC64K
add  "T-ISDN"   TRANS     PPP       TRANS     none      HDLC64K
add  "MLPPP"    TRANS     PPP       TRANS     bnd+cmpr  HDLC64K
add  "PPPHDLC"  TRANS     PPP       TRANS     none      HDLC64K
add  "RAWHDLC"  TRANS     TRANS     TRANS     none      HDLC64K
add  "T-DSL"    TRANS     PPP       PPPoE     none      ETH
add  "PPPOE"    TRANS     PPP       PPPoE     none      ETH
add  "IPOE"     ETHER     TRANS     TRANS     none      ETH
add  "DHCPOE"   ETHER     DHCP      TRANS     none      ETH
add  "V.24_DEF"  TRANS     APPP      TRANS     none      SERIAL
add  "ARCOR"    TRANS     PPP       TRANS     none      HDLC64K
cd /Setup/WAN/PPP
del *
add  "DEFAULT"         PAP       ""        0     5     ""
add  "ARCOR"           none      "arcor"   0     5     "arcor"
set /Setup/LAN/Connector 32
set /Setup/TCP-IP/Intranet-Address 192.168.2.101
cd /Setup/IP-Router/IP-Routing-Table
del *
add  192.168.0.0      255.255.0.0      0        "0.0.0.0"         0         No
add  172.16.0.0       255.240.0.0      0        "0.0.0.0"         0         No
add  10.0.0.0         255.0.0.0        0        "0.0.0.0"         0         No
add  224.0.0.0        224.0.0.0        0        "0.0.0.0"         0         No
add  255.255.255.255  0.0.0.0          0        "ARCOR"           0         on
set /Setup/DHCP/Operating No
cd /Setup/Config/Access-Table
set  LAN     Yes     Yes     Yes     Yes     Yes     Yes         Yes
set  WAN     No      No      No      No      No      No          No
set /Setup/Mail/SMTP-Port 0
set /Setup/Mail/POP3-Port 0
set /Setup/Mail/Send-Again-(min.) 0
set /Setup/Mail/Hold-Time-(hrs.) 0
set /Setup/Mail/Buffers 0
flash Yes

# done
exit
```

From this example it is possible to recognize the behavior of the scriptthat was generated with the command `readscript`:

- The parameters with values different from the default settings are displayed
- The values in the tables are deleted (del *) and replaced with the current values in the configuration (add *).
- Those table entries or values that cannot be left empty are directly changed with the ‘Set’ command.

Note: For table lines or strings containing passwords, the passwords are displayed in clear text, as this is the format required by the Telnet interface. With the generated script you can configure a OpenBAT device exactly like the original device. As these scripts can be very long in some cases, you can also generate scripts for specific parts of the configuration. To do this, you first switch to the directory containing the configuration that you want to record (e.g. `cd set/ip router/firewall` for the firewall settings). Then execute the command “readscript”. Alternatively, enter the path directly with the command “readscript” as a PATH parameter (e.g. `readscript set/ip router/firewall`). In both cases, only the firewall settings that have been changed will be recorded in the script.

The following options can be used with the readscript command:

- -d (default): The commands for modifying parameters that are set to the factory settings will also be listed. These long scripts are useful for transferring configurations between different types of devices, or between devices with different firmware versions, as the factory settings can vary.
- -n (numeric): This suffix causes the paths to be output in the numeric form of the SNMP description, instead of in plain text. This also facilitates the transfer of scripts between devices with different firmware versions, as the path names may change but the SNMP tree generally remains unchanged.

  - -c (comment): In combination with -d and -n, this parameter generates additional comments that make the script easier to read. For the parameter -d, every command combination that sets a default value is marked with # default value. With -n, each numeric path is supplemented with its plain text equivalent.
  - -m (minimize): This parameter removes any gaps in the script, making it more compact.

- #
  The # character followed by a space at the start of a line comprise the first characters of a comment. Any subsequent characters to the end of the line will be ignored.

  Note: Insert a space after the # symbol.

- `del *`
  This command deletes the table in the branch of the menu tree defined with Path.
  Syntax: `del [PATH]`*

- `default`
  This command resets individual parameters, tables or entire menu trees to their factory settings.
  Syntax: `default [-r] [PATH`]

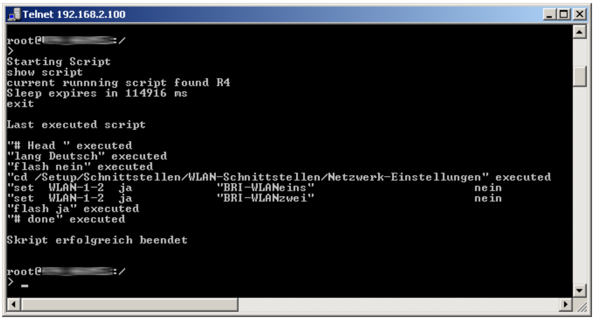
  This command resets the parameters addressed with PATH to their factory settings. If PATH refers to a branch of the menu tree, enter the option “-r” (recursive).

  Login to the console with write permission to execute this command.

- `beginscript`
  The `beginscript` command sets a console session to the script mode. In this state, commands entered are not transferred directly to the configuration RAM of the OpenBAT device, but initially to the script memory of the device. The “exit” command is required to transfer the commands exclusively via a script session to the configuration RAM and execute them there.

  Note: Login to the console with write permission to execute this command.

- `show script`
  The command show script displays the content of the most recently executed script and an overview of the currently running scripts. The names displayed in this output can be used to interrupt scripts early.



```
root@[redacted]:/
>
Starting Script
show script
current runnning script found R4
Sleep expires in 114916 ms
exit

Last executed script

"# Head " executed
"lang Deutsch" executed
"flash nein" executed
"cd /Setup/Schnittstellen/WLAN-Schnittstellen/Netzwerk-Einstellungen" executed
"set  WLAN-1-2  ja            "BRI-WLANeins"                     nein
"set  WLAN-1-2  ja            "BRI-WLANzwei"                     nein
"flash ja" executed
"# done" executed

Skript erfolgreich beendet


root@[redacted]:/
> _
```

Note: Log on to the console with write access rights to execute this command.

- `killscript`
  The command killscript deletes the content of a script session that has not yet been executed. The script session is selected by its name.

- `flash Yes/No`
  When configuring a device with scripts, any add-, set- or del- command can lead to an unintentional update of the configuration in flash. To combat this, the update to flash function can be deactivated. After concluding the configuration, this function can be activated again with `flash Yes`. Changes in the RAM configuration are then written to flash. The status `flash Yes/No` is stored globally.

  Note: Log on to the console with write access rights to execute this command.

- `sleep`
  The sleep command allows the processing of configuration commands to be delayed for a certain time period, or to be scheduled for a certain time. Syntax: `sleep [-u] value[suffix]`

  Permissible suffixes are `s`, `m`, or `h` for seconds, minutes, or hours; if no suffix is defined, the units are milliseconds. With the option switch -u, the sleep command accepts times in the formats:
  `MM/DD/YYYY hh:mm:ss` (English)
  `TT.MM.JJJJ hh:mm:ss`(German)

  Note: Times will be accepted if the system time has been set.

The sleep function is useful for a time-delayed reboot when testing an altered configuration, or for a scheduled firmware update for large-scale roll-outs with multiple devices.

11 Managing Rights for Administrators

You can configure each OpenBAT device for a maximum of 16 administrators, all with different access rights.

Note: Along with the administrators set up in the configuration, there is also the “root” administrator with the main password for the device. This administrator always has full rights, and cannot be deleted or renamed. To login as the root administrator, enter the user name “root” in the login window or leave this field empty.

As soon as you have set up a password for the “root” administrator in the configuration of the device, the “Login” button appears when you call up WEBconfig. When you click this, the login window opens. After you have entered the correct user name and password, the main menu of WEBconfig opens. This menu only displays the options that are available to the administrator who is currently logged in.

If at least one more administrator is set up in the admin table, the main menu also contains the “Change administrator” button, which allows you to switch to a different user ID (with different rights, if applicable).

11.1 Administrator Rights

An administrator’s rights are determined by assignments from two different groups:

- Each administrator belongs to a specific administrator group with globally defined group-based access rights.
- Each administrator also is assigned specific function rights that determine the administrator’s ability to perform specific tasks.

11.1.1 Access Rights

Each administrator is a member of one of the following administrator groups:

Description in Telnet/Terminal	Description in LANconfig/WEBconfig	Access
Supervisor	All	Supervisor - member of all group
Admin RW	Restricted and trace	Local administrator with read and write access
Admin-RW limit	Restricted	Local administrator with read and write access but without trace rights
Admin RO	Read and trace	Local administrator with read access but no write access
Admin-RO limit	Read only	Local administrator with read access but no write access and no trace rights
None	None	No access to the configuration

- Supervisor:
  Has full access to the configuration.

- Local administrator with read and write access:
  Also has full access to the configuration, although the following options are prohibited:
  - Upload firmware to the device
  - Upload configuration onto the device
  - Configuration by LANconfig

  Note: Local administrators with write access can also edit the admin table. However, a local administrator can exclusively change or create entries for users with the same or fewer rights than himself. It follows that a local administrator cannot create a supervisor access and assign himself those rights.

- Local administrator with read and write rights but without trace rights:
  Also has full access to the configuration, although the following options are prohibited:
  - Upload firmware to the device
  - Upload configuration onto the device
  - Configuration by LANconfig
  - Trace output via Telnet or LANmonitor

  Note: Local administrators with write access but without trace rights cannot create administrators with trace rights.

- Local administrator with read access:
  Can read the configuration with Telnet or a terminal program, but cannot change any values. The administrators can be assigned certain configuration options via their function rights.

- None:
  Cannot read the configuration. The administrators can be assigned certain configuration options via their function rights.

11.1.2 Function Rights

Function rights can be used to grant the following options to users:

- Basic wizard
- Internet wizard
- RAS wizard
- WLAN linktest
- Rollout wizard
- Adjustment of date and time
- Search of further devices in LAN
- SSH client
- Security wizard
- Provider selection
- LAN-LAN wizard
- WLAN wizard
- Content filter wizard

11.2 Administrators’ Access via TFTP and SNMP

In addition to using LANconfig, WEBconfig, Telnet, terminal programs or secure shell (SSH) access, administrators can also access a OpenBAT via tftp or SNMP.

11.2.1 TFTP Access

In tftp, the administrator name and password are coded in the source (tftp read request) or target file names (tftp write request). The file name is made up of either the master password and the command to be executed, or the combination of administrator name and password (separated by a colon), with the command as a suffix. Therefore, a command sent via tftp looks like this:

```
<Master password><Command>
```

or...

```
<User name>:<Password>@<Command>
```

In the following examples, the OpenBAT device has the configuration:

- Address = “mydevice.intern”
- Master password = “RootPwd”
- Administrator name = “LocalAdmin”
- Administrator password = “Admin”

Read the configuration from the device (supervisor):

```
tftp mydevice.intern GET
RootPwdreadconfig mydevice.lcf
```

Write the configuration to the device (supervisor):

```
tftp mydevice.intern PUT
mydevice.lcf RootPwdwriteconfig
```

Read the device MIB from the device (for local administrator):

```
tftp mydevice.intern GET localadmin:Admin@readmib
mydevice.mib
```

For the menus and available commands, the same limitations on rights apply as with Telnet.

11.2.2 SNMP Access

For the administration of networks with the help of SNMP tools such as HP OpenView, the various levels of administrator access can be used for the precise control of rights.

Under SNMP, administrator name and password are coded as part of the ‘community’. Permissible selections include:

- the 'public' community name
- the master password
- a combination of user name and password divided by a colon

Note: The 'public' community setting corresponds with the rights of a local administrator with read-only access, as long as the SNMP read access without password is enabled. If this access is prohibited, then the 'public' community setting denies access to all menus.

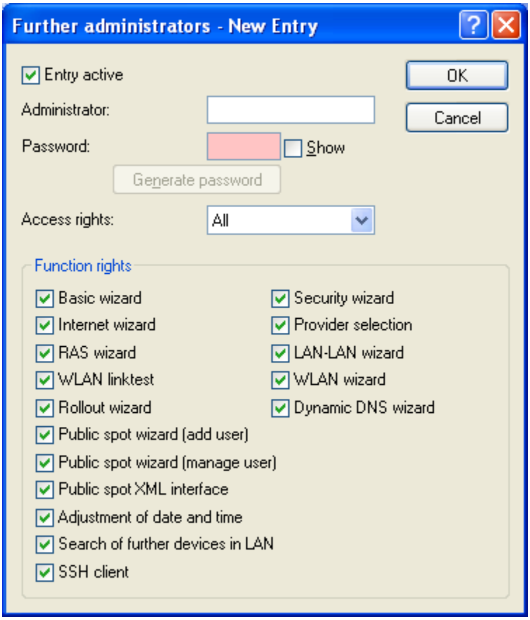
Otherwise, the same limitations on rights apply for the menus as with Telnet.

11.2.3 Configuring User Rights

LANconfig and WEBconfig

To access a list of administrators, where you can edit the rights of a selected administrator account in LANconfig, follow these steps:

- □ Open the configuration file for a device in LANconfig by highlighting the device, then selecting `Device : Configure`.
- □ Open the `Configuration : Management  Admin` dialog, and click ‘Further administrators...’ to open that window.
- □ In the ‘Further administrators’ window, either click ‘Add...’ to create a new administrator account, or select an existing entry and click ‘Edit...’ to open the ‘Edit Entry’ dialog:



☑ Entry active

Administrator:

Password: ☐ Show

Access rights: All

Function rights

☑ Basic wizard
☑ Internet wizard
☑ RAS wizard
☑ WLAN linktest
☑ Rollout wizard
☑ Public spot wizard (add user)
☑ Public spot wizard (manage user)
☑ Public spot XML interface
☑ Adjustment of date and time
☑ Search of further devices in LAN
☑ SSH client
☑ Security wizard
☑ Provider selection
☑ LAN-LAN wizard
☑ WLAN wizard
☑ Dynamic DNS wizard

To access the administrator accounts in WEBconfig, the path is virtually the same as in LANconfig:

`Configuration : Management : Admin`

In both LANconfig and WEBconfig, you can edit the name, password, access rights, and function rights for each administrator account. You can also enable and disable the account. By disabling the account, you can save the administrator account configuration for future use.

Telnet or Terminal Program

In Telnet or a terminal program, you will find the administrator accounts in the same location as for WEBconfig:

```
Configuration : Management :Admin
```

Administrator group access rights are described above (see page 164). Function rights are represented by the following hexadecimal values:

Value	Access
0x00000001	The user can run the Basic Settings Wizard
0x00000002	The user can run the Security Wizard
0x00000004	The user can run the Internet Wizard
0x00000008	The user can run the Wizard for selecting Internet providers
0x00000010	The user can run the RAS Wizard
0x00000020	The user can run the LAN-LAN Coupling Wizard
0x00000040	The user can set the date and time
0x00000080	The user can search for additional devices
0x00000100	The user can run the WLAN Link test
0x00000200	The user can run the a/b Wizard
0x00000400	The user can run the WTP Assignment Wizard
0x00000800	The user can run the Public Spot Wizard
0x00001000	The user can run the WLAN Wizard
0x00002000	The user can run the Rollout WizardThe user can run the WLAN Wizard
0x00004000	The user can run the Dynamic DNS Wizard
0x00008000	The user can run the VoIP Call Manager Wizard
0x00010000	The user can run the WLC Profile Wizard

The entry for an administrator account is the sum of the first, second and third columns from the right. If, for example, the user is to receive rights to use the ’Security Wizard’, ’Selection of Internet provider’, ’RAS Wizard’, ’Change time’ and ’WLAN Link Test’, then the resulting values are as follows:

Third Column	Second Column	First Column
WLAN linktest = 1	RAS Wizard = 1 Change Time = 4	Security Wizard = 2 Internet Provider = 8
Total = 1	Total = 5	Total = a

In the above example, the function rights value equals ‘0x0000015a’.

Examples:

The following command sets up a new user in the table who, as local administrator ’Mueller’ with the password ’BW46zG29’, can select the Internet provider. The user will be activated immediately:

```
set Mueller BW46zG29 yes Admin-RW 00000008
```

The following command extends the function rights such that user ’Mueller’ can also run the WLAN link test (the asterisks stand for the values which are not to be changed):

```
set Mueller * * * 00000108
```

11.2.4 TCP Port Tunnel

In some cases it can be useful to enable temporary remote access to a OpenBAT device in a LAN via http (TCP port 80) or TELNET (TCP port 23). For example, if a question arises regarding the performance of a device, technical support personnel can provide better assistance if they can directly access the device in the customer’s LAN.

However, the standard method for accessing LAN devices via inverse masquerading (port forwarding) sometimes requires a special configuration of the firewall. As an alternative to port forwarding, you can set up temporary access for remote maintenance that automatically closes again after a specific period of inactivity. To enable this access, the support staff member requiring access to a device in the network creates a “TCP/http tunnel” via TCP port 80.

Note: This access in only valid for the IP address from which the tunnel was created. This type of access to devices in the network is not transferable.

Configuring the Device for TCP/HTTP Tunnels

To configure the OpenBAT device for a TCP/http tunnel, call up the following dialog in WEBconfig:

```
HiLCOS menu tree : Setup : HTTP
```

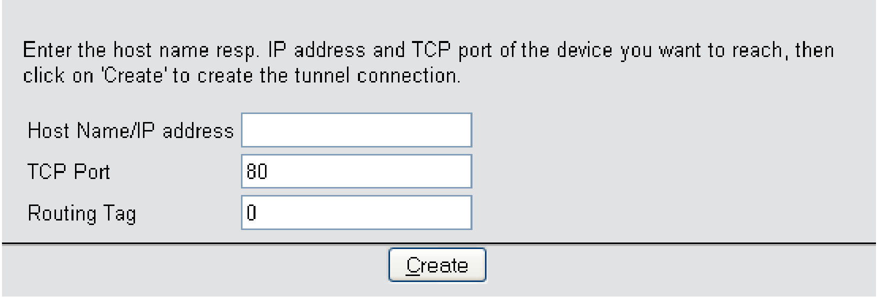
Configure the following properties:

- **Max. tunnel connections:**
  Maximum number of simultaneously active TCP/http tunnels.
- **Tunnel idle timeout:**
  Life span of a tunnel without activity. After this time expires, the tunnel closes automatically unless it is being used to transfer data.

Creating a TCP/HTTP Tunnel

To create a TCP/http tunnel, navigate to the following dialog in WEBconfig:

```
Extras : Create TCP/HTTP Tunnel
```



Enter the host name resp. IP address and TCP port of the device you want to reach, then click on 'Create' to create the tunnel connection.

Host Name/IP address	
TCP Port	80
Routing Tag	0

Configure the following properties:

- **Host name/IP address:**
  Enter the name or IP address of the device that is to be temporarily available via http
- **TCP Port:**
  Select a port for the http tunnel.
- **Routing Tag:**
  If necessary, select a routing tag.

Note: In addition to http or https-based access, remote maintenance can also be based on any other TCP service such as telnet connections (TCP port 23) or SSH (TCP port 22).

The newly created HTTP tunnel is deleted automatically if the tunnel remains inactive for the duration of the tunnel idle timeout. To delete the tunnel earlier, access the list of active tunnels and delete the one you no longer require at the following WEBconfig location:

```
HiLCOS-Menu Tree : Status : TCP-IP : HTTP :
Active Tunnels
```

Note: While active TCP connections in this tunnel will continue to exist for a short time, new connections cannot be established.

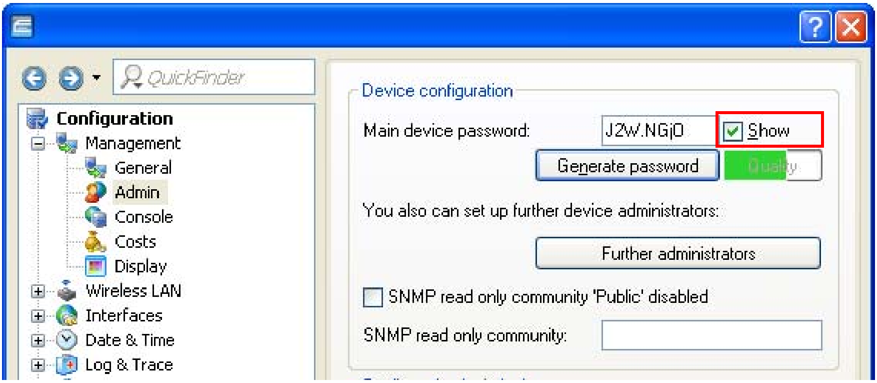
11.3 Secure Passwords

Access to all the passwords and keys stored in the device is secured by an additional password. The device only displays this data in clear text after this password is entered.
The supervisor has unrestricted access to all the passwords. You can withdraw this access right explicitly from other administrators by assigning the administration type **Admin NP** .
For access via all connection methods (LANconfig, WEBconfig, Telnet, SSH), the device checks the access rights of the administrator logged in and, if applicable, shows the passwords in clear text. In the configuration management, LANconfig also acts based on the access rights and correspondingly displays the passwords in clear text or obscured.
In LANconfig, you will find these settings under
`Configuration:Management:Admin:Other Administrators`

Note: In script files, passwords are generally in clear text. Therefore, saving these scripts in an unprotected area amounts to a security breach.

11.3.1 Generating Secure Passwords Automatically

LANconfig provides the option to automatically generate a password at all points in the configuration, which require the input of a password or a passphrase.



Device configuration

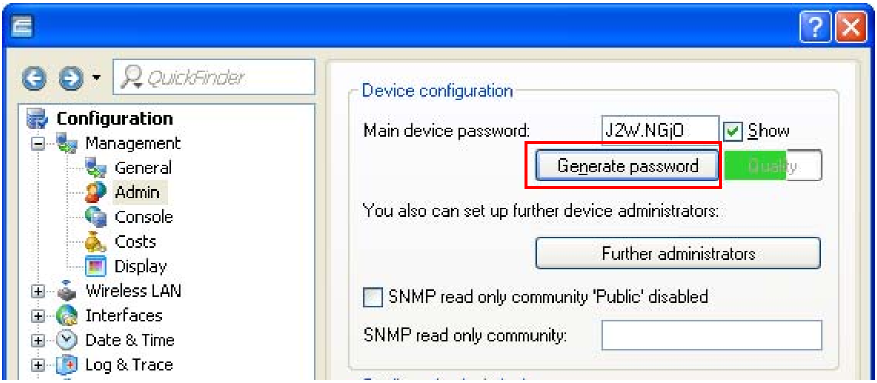
Main device password: J2W.NGj0 ☑ Show

You also can set up further device administrators:

☐ SNMP read only community 'Public' disabled

SNMP read only community:

Enable the option "Show" next to the box for entering the password. Then click on the button "Generate password" to create a password suggestion.



Device configuration

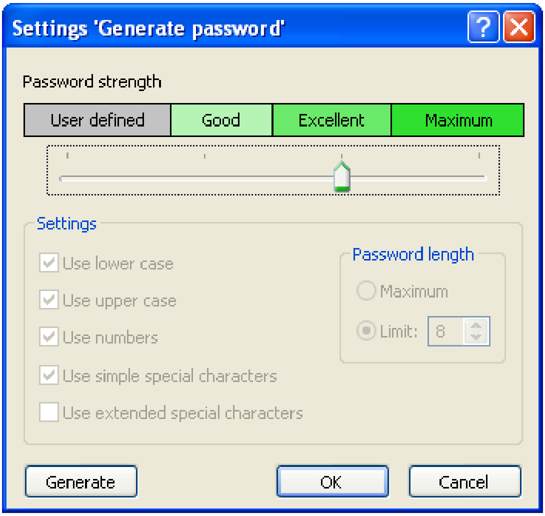
Main device password: J2W.NGj0 ☑ Show

You also can set up further device administrators:

☐ SNMP read only community 'Public' disabled

SNMP read only community:

Optionally click the arrow next to the "Generate password" button to open the dialog box for the password policy settings.



Settings 'Generate password'

Password strength

User defined | Good | Excellent | Maximum

Settings

☑ Use lower case

☑ Use upper case

☑ Use numbers

☑ Use simple special characters

□ Use extended special characters

Password length

○ Maximum

● Limit: 8

Use the slider to set the desired password strength. With the "User defined" setting, you can define the maximum password length and the required character types. The settings "Good", "Very good" and "Maximum" are predefined settings with reasonable, non-modifiable values.

After making your changes, click on the "Generate password" button again to create a new password proposal in line with your password guidelines.

Note: LANconfig stores the current settings in this dialog box for the current user.

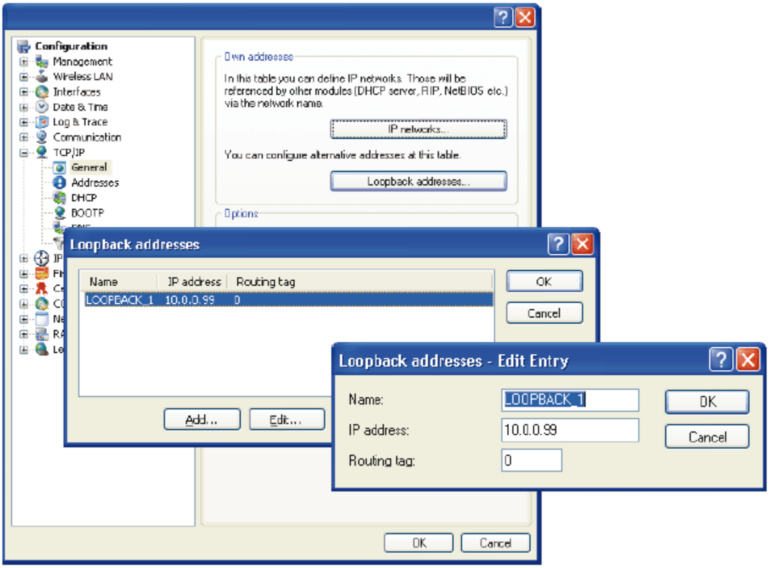
12 Managing Networks with Loopback Addresses

You have the option of configuring up to 16 loopback addresses in a OpenBAT device, by means of which the device can be addressed. This can be an advantage when managing larger network structures. To use the loopback addresses for certain networks (e.g. in connection with advanced routing and forwarding), routing tags can be assigned to these addresses. To make them easier to identify in other configuration units, the loopback addresses are also given a freely definable name.

To manage loopback addresses for a OpenBAT device:

☐ Open the LANconfig device configuration file to the following dialog: `Configuration : TCP/IP : General`, and click ‘Loopback addresses...’

☐ In the ‘Loopback addresses’ window, click ‘Add...’ to create a new loopback address, or select an existing entry and click ‘Edit...’ to modify an existing loopback address.



In this table you can define IP networks. Those will be referenced by other modules (DHCP server, RIP, NetBIOS etc.) via the network name.

You can configure alternative addresses at this table.

Name	IP address	Routing tag
LOOPBACK_1	10.0.0.99	0

Name: LOOPBACK_1

IP address: 10.0.0.99

Routing tag: 0

Configure the following properties for each loopback address:

- Name:
  A freely definable name for the loopback address, up to 16 characters.
- Loopback address:
  The IP address used for this loopback address for the device.
- Routing tag:
  Routing tag of the loopback address. Loopback addresses with the routing tag '0' (untagged) are visible to all networks. Loopback addresses with a different routing tag are only visible to networks with the same routing tag.

12.1 Loopback Addresses with ICMP Polling

Similarly to LCP monitoring, with ICMP polling the device regularly sends requests to a remote site. The device sends ping commands and monitors the responses. In contrast to LCP monitoring, you have the option of freely defining the remote site for the ICMP pings. With one ping to a router in a remote network it is possible to monitor the entire connection, not just the section to the Internet provider.

A ping interval is defined for the remote site in the polling table. Also defined, in the event that replies are missed, is the number of retries before the transmission of a new LCP request. If the transmitter does not receive any reply to the retries, the target for the ping requests is classified as unavailable.

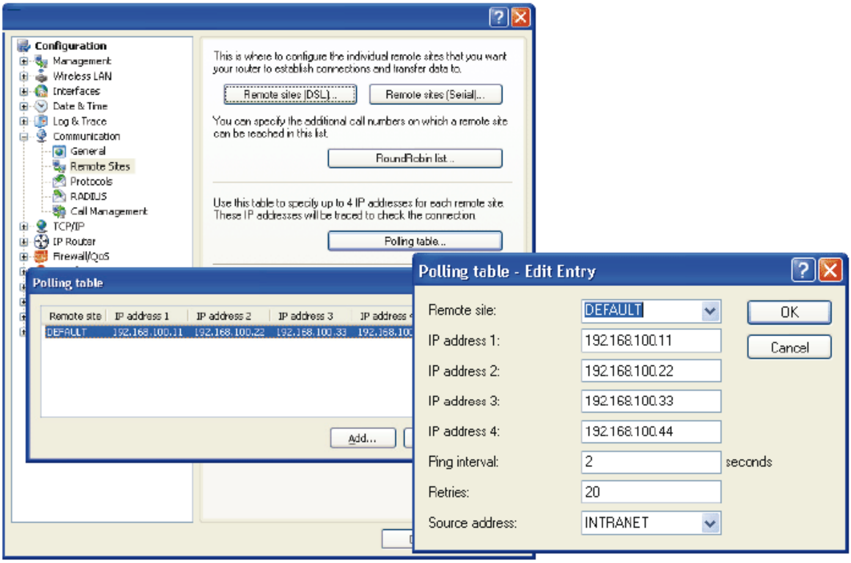
Up to four different IP addresses can be entered for each remote site that will be checked in the remote network in parallel. Only if all of the IP addresses are unavailable is the connection considered to be no longer active.

Note: ICMP polling enables you to monitor an entire connection from end to end.

To configure the polling entries with loopback addresses for a OpenBAT device:

☐ Open the LANconfig device configuration file to the following dialog: `Configuration : Communication : Remote Sites`, and click ‘Polling table...’

☐ In the ‘Polling table’ window, click ‘Add...’ to create a new polling entry, or select an existing entry and click ‘Edit...’ to modify an existing polling entry:



This is where to configure the individual remote sites that you want your router to establish connections and transfer data to.

You can specify the additional call numbers on which a remote site can be reached in this list.

Use this table to specify up to 4 IP addresses for each remote site. These IP addresses will be traced to check the connection.

Remote site	IP address 1	IP address 2	IP address 3	IP address 4
DEFAULT	192.168.100.11	192.168.100.22	192.168.100.33	192.168.100

Remote site: DEFAULT

IP address 1: 192.168.100.11

IP address 2: 192.168.100.22

IP address 3: 192.168.100.33

IP address 4: 192.168.100.44

Ping interval: 2 seconds

Retries: 20

Source address: INTRANET

Configure the following properties for each ICMP polling entry:

- Peer:
  Name of the remote station which is to be checked with this entry.
- IP address 1 - 4:
  IP addresses for targeting with ICMP requests to check the remote site.

  Note: If no IP address that can be checked with a ping is entered for a remote site, then the IP address of the domain name service (DNS) server that was determined during the point to point protocol (PPP) negotiation will be checked.
- Ping interval:
  The time entered into the polling table defines the time interval between ping requests. If the value “0” is entered, then the standard value of 30 seconds applies.

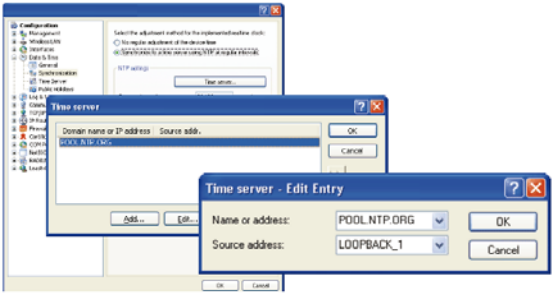
- Retries:
  If no reply to a ping is received, the remote site is checked in shorter intervals of once a second. The number of retries defines how many times these attempts are repeated. If the value “0” is entered, then the standard value of 5 retries applies.
- Loopback address:
  Sender address sent with the ping; this is also the destination for the answering ping.

12.2 Loopback Addresses for Time Servers

OpenBATs can retrieve time information from public time servers via the Internet (NTP server). When defining the time server, the name or IP address of the NTP server being queried by the OpenBAT can be entered, as well as loopback addresses.

To configure time servers with loopback addresses for a OpenBAT device:

- □ Open the LANconfig device configuration file to the following dialog: `Configuration : Date & Time : Synchronization`, and click ‘Time server...’
- □ In the ‘Time server’ window, click ‘Add...’ to create a new entry, or select an existing entry and click ‘Edit...’ to modify it:



Time server

Domain name or IP address | Source addr.
POOL.NTP.ORG

Time server - Edit Entry

Name or address: POOL.NTP.ORG

Source address: LOOPBACK_1

Configure the following properties for each ICMP polling entry:

- ▶ Name
  Name or IP address of the NTP server. The OpenBAT router attempts to reach the servers in the order in which they are entered.
- ▶ Loopback address
  Sender address sent with the NTP request; this is also the destination for the NTP answer.

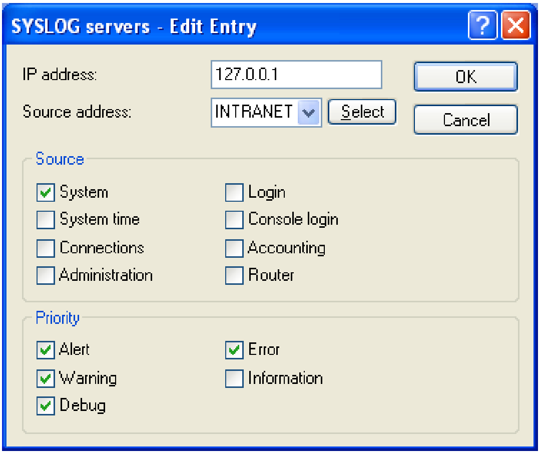
12.3 Loopback Addresses for SYSLOG Servers

You can configure SYSLOG servers to receive SYSLOG messages from the OpenBAT device. SYSLOG servers are configured to receive SYSLOG messages. The messages can be sent via loopback addresses in the OpenBAT device.

To configure a OpenBAT device to send SYSLOG messages to a remote SYSLOG server:

□ Open the LANconfig device configuration file to the following dialog: `Configuration : Log & Trace : General`. Click “SYSLOG servers”.

□ In the ‘SYSLOG servers’ window, click ‘Add...’ to create a new entry. If you want to modify an existing entry, mark the entry and click ‘Edit’.



SYSLOG servers - Edit Entry

IP address: 127.0.0.1

Source address: INTRANET

Source

☑ System
□ System time
□ Connections
□ Administration
□ Login
□ Console login
□ Accounting
□ Router

Priority

☑ Alert
☑ Warning
☑ Debug
☑ Error
□ Information

Configure the following properties for each SYSLOG entry:

- IP address:
  IP address of the SYSLOG client
- Loopback address:
  Sender address entered into the SYSLOG message. No answer is expected to a SYSLOG message.
- Source: Select one or more of the following:
  - System: System messages (boot events, timer system, etc.)
  - Logins: Messages concerning the user's login or logout during the PPP negotiation, and any errors detected during login or logout.
  - System time: Messages about changes to the system time.
  - Console logins: Messages about console logins (Telnet, Outband, etc.), logouts and any errors detected during login.
  - Connections: Messages about establishment and termination of connections and any errors detected (e.g., display trace).
  - Accounting: Accounting information stored after termination of a connection (user, online time, transfer volumes).
  - Administration: Messages on changes to the configuration, remotely executed commands, etc.
  - Router: Regular statistics about the most frequently used services (breakdown per port number) and messages about filtered packets, routing errors, etc.
- Priority: Select one or more of the following:
  - Alert: This is a collection of messages of interest to the administrator (general SYSLOG priority: PANIC, ALERT, CRIT).
  - Error: All event messages which can occur under normal conditions are communicated, e.g. connection errors detected (e.g., general SYSLOG priority: ERROR). No specific action is required by the administrator.
  - Warning: Messages that do not compromise normal operating conditions (general SYSLOG priority: WARNING) are communicated.

– Information: Messages that are of a purely informational character (general SYSLOG priority: NOTICE, INFORM) are communicated.

– Debug: Communication of all debug messages. Debug messages generate large data volumes and can compromise the device's operation. For this reason they should be disabled for normal operations and only used for troubleshooting (general SYSLOG priority: DEBUG).

13 Monitoring the LAN

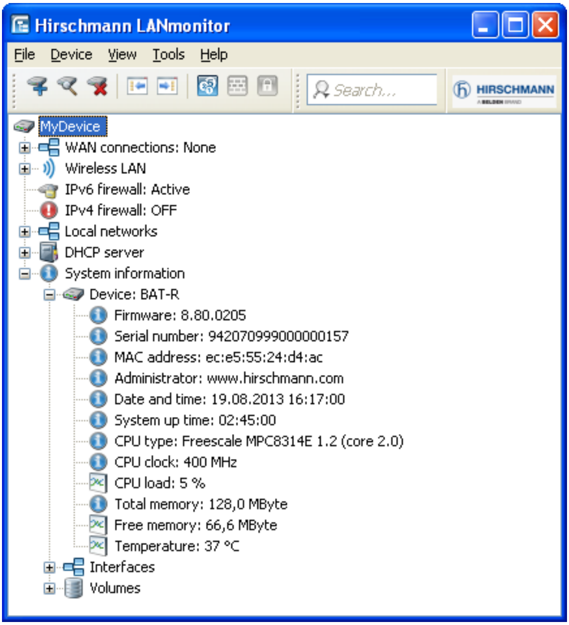
You use the LANmonitor software tool for the following tasks:

- To display the status of the individual OpenBAT devices in the network
- To monitor traffic at the various interfaces of the OpenBAT device
- To gather information about configurable device settings that are used to optimize the data traffic

Note: Monitoring with LANmonitor is only possible for devices that are connected via their IP address. LANmonitor is unable to access devices that are connected via their serial interface.

13.1 Display Functions in LANmonitor

LANmonitor supports the administration of the OpenBAT applications by offering a range of functions that simplify the surveillance of devices at widely dispersed locations. The overview of devices monitored by LANmonitor displays information about the status of the devices:

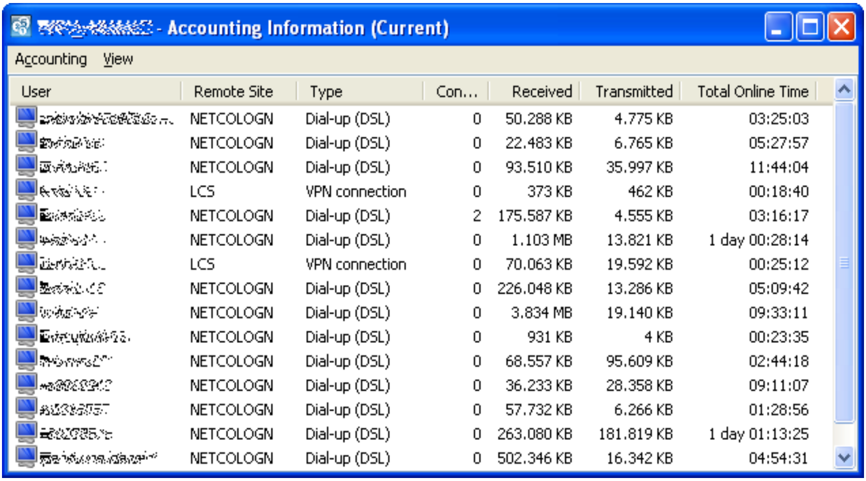


MyDevice
- WAN connections: None
- Wireless LAN
- IPv6 firewall: Active
- IPv4 firewall: OFF
- Local networks
- DHCP server
- System information
  - Device: BAT-R
    - Firmware: 8.80.0205
    - Serial number: 942070999000000157
    - MAC address: ec:e5:55:24:d4:ac
    - Administrator: www.hirschmann.com
    - Date and time: 19.08.2013 16:17:00
    - System up time: 02:45:00
    - CPU type: Freescale MPC8314E 1.2 (core 2.0)
    - CPU clock: 400 MHz
    - CPU load: 5 %
    - Total memory: 128,0 MByte
    - Free memory: 66,6 MByte
    - Temperature: 37 °C
  - Interfaces
  - Volumes

The information that can be taken from this overview includes details about active WAN connections, the five most recent firewall messages, and system information about charges and online times.

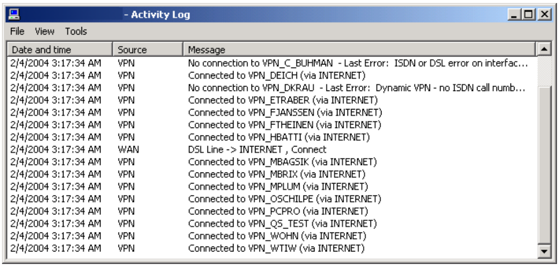
Right-clicking on a device in LANmonitor opens a context menu with additional information:

- Accounting information
  The accounting information is a protocol of the connections from each station in the LAN to remote sites in the WAN. The detailed information recorded includes:
  – Name or IP address of the station
  – Remote station used to establish the connection
  – Type of connection, e.g. digital subscriber line (DSL)
  – Number of connections
  – Data volume transmitted and received
  – total online time



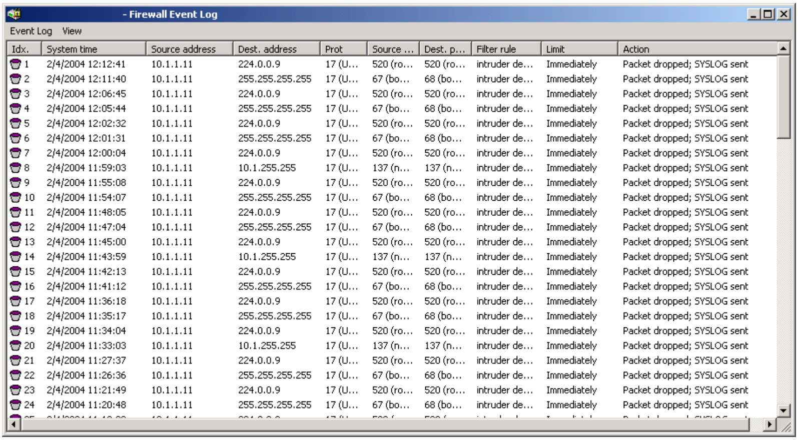
User	Remote Site	Type	Con...	Received	Transmitted	Total Online Time
[redacted]	NETCOLOGN	Dial-up (DSL)	0	50.288 KB	4.775 KB	03:25:03
[redacted]	NETCOLOGN	Dial-up (DSL)	0	22.483 KB	6.765 KB	05:27:57
[redacted]	NETCOLOGN	Dial-up (DSL)	0	93.510 KB	35.997 KB	11:44:04
[redacted]	LCS	VPN connection	0	373 KB	462 KB	00:18:40
[redacted]	NETCOLOGN	Dial-up (DSL)	2	175.587 KB	4.555 KB	03:16:17
[redacted]	NETCOLOGN	Dial-up (DSL)	0	1.103 MB	13.821 KB	1 day 00:28:14
[redacted]	LCS	VPN connection	0	70.063 KB	19.592 KB	00:25:12
[redacted]	NETCOLOGN	Dial-up (DSL)	0	226.048 KB	13.286 KB	05:09:42
[redacted]	NETCOLOGN	Dial-up (DSL)	0	3.834 MB	19.140 KB	09:33:11
[redacted]	NETCOLOGN	Dial-up (DSL)	0	931 KB	4 KB	00:23:35
[redacted]	NETCOLOGN	Dial-up (DSL)	0	68.557 KB	95.609 KB	02:44:18
[redacted]	NETCOLOGN	Dial-up (DSL)	0	36.233 KB	28.358 KB	09:11:07
[redacted]	NETCOLOGN	Dial-up (DSL)	0	57.732 KB	6.266 KB	01:28:56
[redacted]	NETCOLOGN	Dial-up (DSL)	0	263.080 KB	181.819 KB	1 day 01:13:25
[redacted]	NETCOLOGN	Dial-up (DSL)	0	502.346 KB	16.342 KB	04:54:31

- Activity log
  The activity log is a detailed list of the connections via WAN, WLAN, and a list of firewall activities. The detailed information recorded includes:
  – Date and time
  – Source
  – Message



Date and time	Source	Message
2/4/2004 3:17:34 AM	VPN	No connection to VPN_C_BUHMAN - Last Error: ISDN or DSL error on interfac...
2/4/2004 3:17:34 AM	VPN	Connected to VPN_DEICH (via INTERNET)
2/4/2004 3:17:34 AM	VPN	No connection to VPN_DKRAU - Last Error: Dynamic VPN - no ISDN call numb...
2/4/2004 3:17:34 AM	VPN	Connected to VPN_ETRABER (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_FJANSSEN (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_FTHEINEN (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_HBATTI (via INTERNET)
2/4/2004 3:17:34 AM	WAN	DSL Line -> INTERNET , Connect
2/4/2004 3:17:34 AM	VPN	Connected to VPN_MBAGSIK (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_MBRIX (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_MPLUM (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_OSCHILPE (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_PCPRO (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_QS_TEST (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_WOHN (via INTERNET)
2/4/2004 3:17:34 AM	VPN	Connected to VPN_WTIW (via INTERNET)

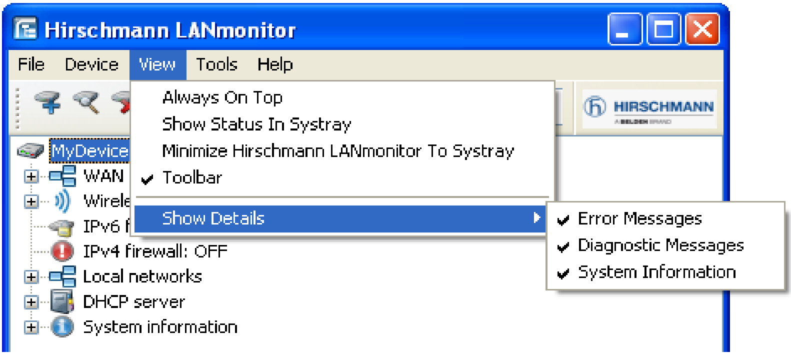
- Firewall actions log
  The firewall actions log lists the last 100 actions taken by the firewall. The detailed information recorded includes:
  – Time
  – Source and destination address
  – Protocol with source and destination port
  – Activated filter rule and exceeded limit
  – Action carried out



Idx.	System time	Source address	Dest. address	Prot	Source ...	Dest. p...	Filter rule	Limit	Action
1	2/4/2004 12:12:41	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
2	2/4/2004 12:11:40	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
3	2/4/2004 12:06:45	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
4	2/4/2004 12:05:44	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
5	2/4/2004 12:02:32	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
6	2/4/2004 12:01:31	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
7	2/4/2004 12:00:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
8	2/4/2004 11:59:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
9	2/4/2004 11:55:08	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
10	2/4/2004 11:54:07	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
11	2/4/2004 11:48:05	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
12	2/4/2004 11:47:04	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
13	2/4/2004 11:45:00	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
14	2/4/2004 11:43:59	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
15	2/4/2004 11:42:13	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
16	2/4/2004 11:41:12	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
17	2/4/2004 11:36:18	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
18	2/4/2004 11:35:17	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
19	2/4/2004 11:34:04	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
20	2/4/2004 11:33:03	10.1.1.11	10.1.255.255	17 (U...	137 (n...	137 (n...	intruder de...	Immediately	Packet dropped; SYSLOG sent
21	2/4/2004 11:27:37	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
22	2/4/2004 11:26:36	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent
23	2/4/2004 11:21:49	10.1.1.11	224.0.0.9	17 (U...	520 (ro...	520 (ro...	intruder de...	Immediately	Packet dropped; SYSLOG sent
24	2/4/2004 11:20:48	10.1.1.11	255.255.255.255	17 (U...	67 (bo...	68 (bo...	intruder de...	Immediately	Packet dropped; SYSLOG sent

13.2 Expanded Display Options

You can expand the display of monitoring information presented in LANmonitor, by clicking `View : Show Details`, then activating the individual expanded display options:



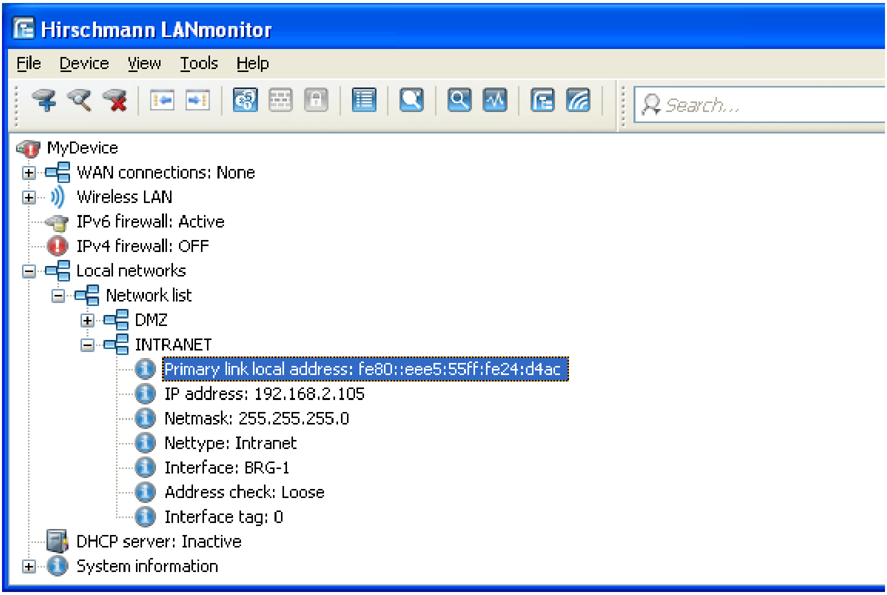
The additional display options include:

- Error messages
- Diagnostic messages
- System information

Note: Many important details about the status of the OpenBAT device are only displayed when the system information display is activated. This includes, for example, the ports and the call charge management.

13.2.1 Display Local IPv6 Addresses

As of HiLCOS version 8.80, LANmonitor can display the IPv6 addresses of local networks. This display function is available in various places within the menu.

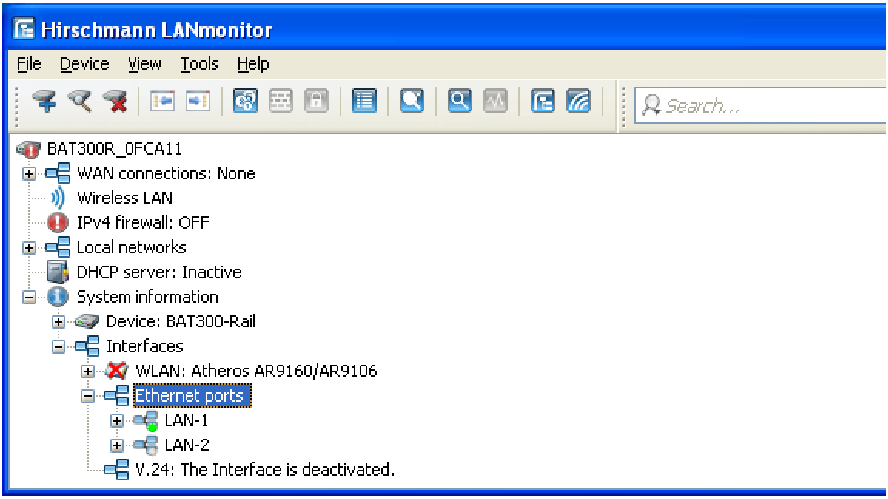


MyDevice
WAN connections: None
Wireless LAN
IPv6 firewall: Active
IPv4 firewall: OFF
Local networks
Network list
DMZ
INTRANET
Primary link local address: fe80::eee5:55ff:fe24:d4ac
IP address: 192.168.2.105
Netmask: 255.255.255.0
Nettype: Intranet
Interface: BRG-1
Address check: Loose
Interface tag: 0
DHCP server: Inactive
System information

13.2.2 Displaying the Active Ethernet Ports

As of HiLCOS version 8.80, LANmonitor allows you to display the operating status of the Ethernet ports.

The menu item `System information:Interfaces:Ethernet ports` shows you whether ports are in operation and, if so, which network the port is assigned to (e.g. LAN-1 after the port name).

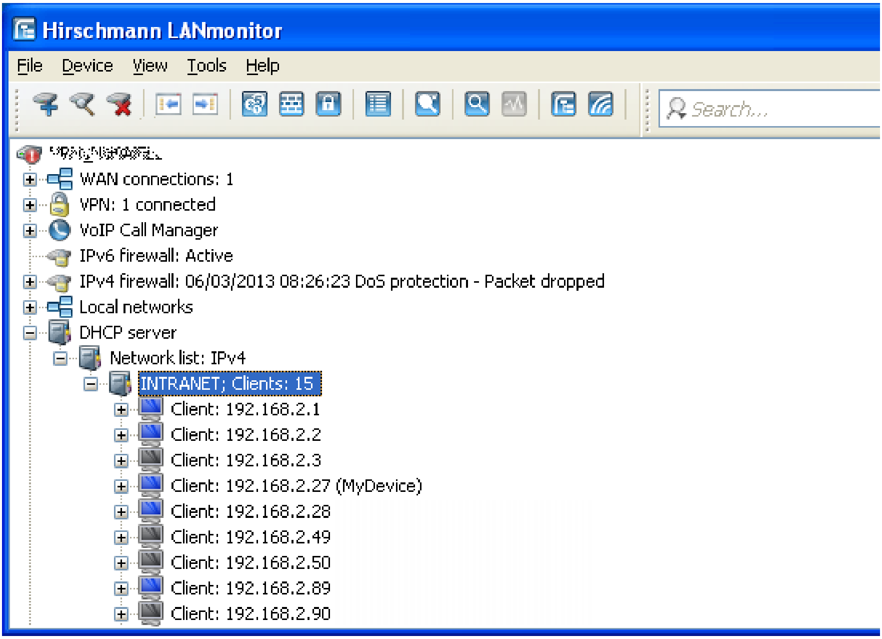


BAT300R_0FCA11
WAN connections: None
Wireless LAN
IPv4 firewall: OFF
Local networks
DHCP server: Inactive
System information
Device: BAT300-Rail
Interfaces
WLAN: Atheros AR9160/AR9106
Ethernet ports
LAN-1
LAN-2
V.24: The Interface is deactivated.

13.2.3 Displaying the DHCP assignment

As of HiLCOS version 8.80, the LANmonitor menu item "DHCP server" displays the connection status of the individual DHCP clients by the color of the corresponding device icon.

- A blue icon shows DHCP clients which are active in the network.
- A gray icon shows DHCP clients which are not currently active in the network (e.g. switched off or disconnected), but which still have a valid DHCP assignment.

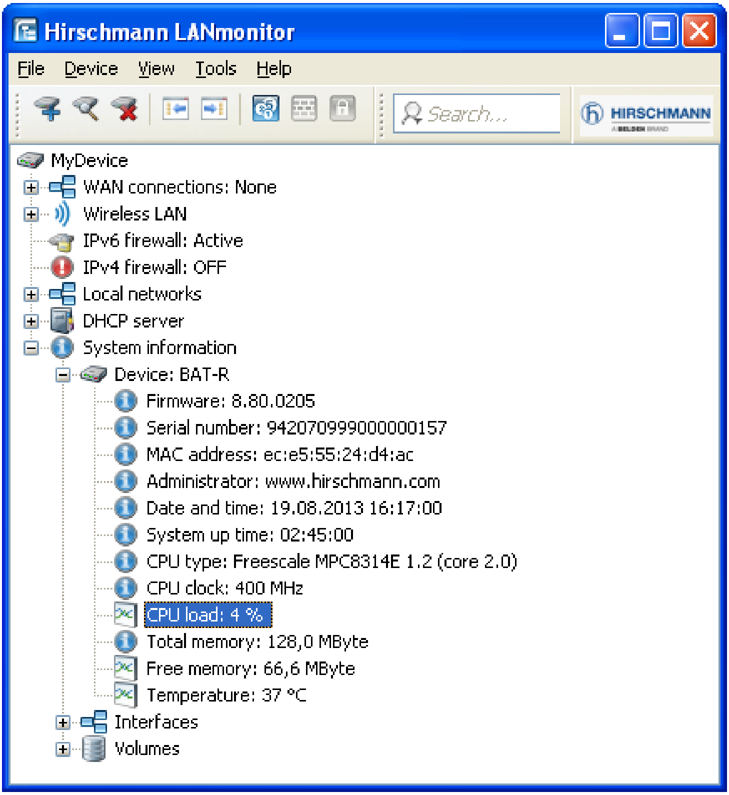


```
[redacted]
+ WAN connections: 1
+ VPN: 1 connected
+ VoIP Call Manager
  IPv6 firewall: Active
+ IPv4 firewall: 06/03/2013 08:26:23 DoS protection - Packet dropped
+ Local networks
- DHCP server
  - Network list: IPv4
    - INTRANET; Clients: 15
      + Client: 192.168.2.1
      + Client: 192.168.2.2
      + Client: 192.168.2.3
      + Client: 192.168.2.27 (MyDevice)
      + Client: 192.168.2.28
      + Client: 192.168.2.49
      + Client: 192.168.2.50
      + Client: 192.168.2.89
      + Client: 192.168.2.90
```

Note: DHCP clients for some operating systems such as Android do not submit a device name. In this case, LANmonitor displays the MAC address of the DHCP client only. This behavior may be undesirable with a large number of clients. To display a device name in these cases, enter the MAC address of the DHCP client with the desired device name into the BOOTP table on the DHCP server.

13.3 Querying CPU and Memory Utilization via SNMP

You can query the CPU and memory utilization of the OpenBAT device via SNMP or display it in LANmonitor.



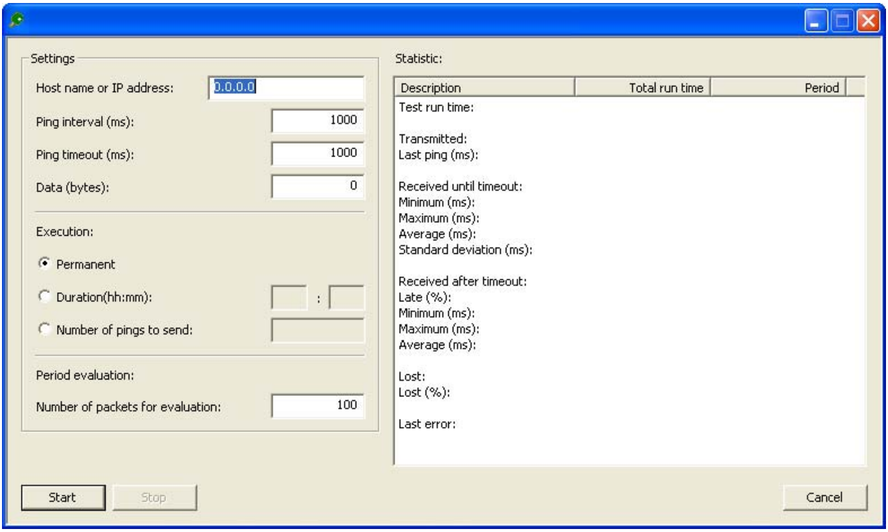
MyDevice
WAN connections: None
Wireless LAN
IPv6 firewall: Active
IPv4 firewall: OFF
Local networks
DHCP server
System information
Device: BAT-R
Firmware: 8.80.0205
Serial number: 942070999000000157
MAC address: ec:e5:55:24:d4:ac
Administrator: www.hirschmann.com
Date and time: 19.08.2013 16:17:00
System up time: 02:45:00
CPU type: Freescale MPC8314E 1.2 (core 2.0)
CPU clock: 400 MHz
CPU load: 4 %
Total memory: 128,0 MByte
Free memory: 66,6 MByte
Temperature: 37 °C
Interfaces
Volumes

13.4 Connection Diagnosis with LANmonitor

LANmonitor can be used to check the connection quality between stations in the LAN, WAN or WLAN. LANmonitor sends pings from the computer on which it is installed to the remote site at regular intervals. The responses it receives are the basis for a compiled report.

To test the parameters and display the results in LANmonitor, open the ‘Ping’ dialog, either by:

- Selecting `Tools : Ping`, or
- Selecting a device in the LANmonitor list, then selecting `Device : Ping...`



Settings

Host name or IP address: 0.0.0.0

Ping interval (ms): 1000

Ping timeout (ms): 1000

Data (bytes): 0

Execution:

● Permanent

○ Duration(hh:mm): :

○ Number of pings to send:

Period evaluation:

Number of packets for evaluation: 100

Statistic:

Description	Total run time	Period
Test run time:		
Transmitted:		
Last ping (ms):		
Received until timeout:		
Minimum (ms):		
Maximum (ms):		
Average (ms):		
Standard deviation (ms):		
Received after timeout:		
Late (%):		
Minimum (ms):		
Maximum (ms):		
Average (ms):		
Lost:		
Lost (%):		
Last error:		

13.4.1 Ping Configuring

Configure the ping using the following parameters. The following information can be entered for each different network device (servers, clients, routers, printers, etc.) which can be reached via LAN, WAN or WLAN:

- Host name or IP address
  The remote station which is to be queried is entered here.
- Ping interval
  The time interval, in ms, between two consecutive pings.

  Note: The interval between two pings cannot be less than the packet transmission time, i.e. before sending a ping, the previous ping must have been answered or the ping timeout must have expired.
- Ping timeout
  The wait interval for the response to a ping to arrive [ms]. If this time expires and no response is received, then the ping is assumed to be lost.
- Data
  The size of a ping packet [bytes]. A ping is an ICMP packet which is generally transmitted without any content, i.e. it is just a header. To increase the load of the packets used for testing a connection, a payload can be created artificially. The overall packet size then consists of an IP header (20 bytes), an ICMP header (8 bytes) and the payload.

  Note: The packets will be fragmented if the payload of the ICMP packets exceeds the maximum IP packet size.
- Execution
  Repeat mode for the ping command.

13.4.2 Ping Evaluation

The right-hand portion of the ‘Ping’ dialog displays the results of the ping test. The first column shows the sum values over the entire test; the second column shows only the values collected over the evaluation period, i.e. the sum of the most recent packets. Unanswered pings are not included in the evaluation.

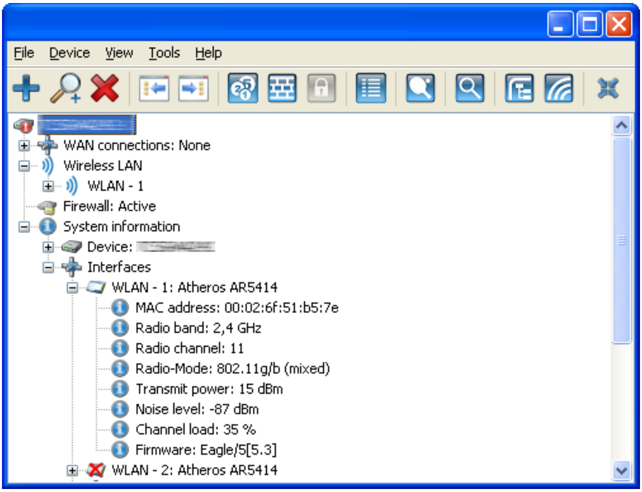
The following information is displayed for evaluation:

- Test run time
  - The total run time [hr./ min./ sec.]
- Transmitted
  - Total number of pings sent
  - Run time of the last ping [ms]
- Received until timeout
  - The number of pings answered in the timeout period
  - Minimum runtime
  - Maximum runtime
  - Average
  - Standard deviation from the mean run time
- Received after timeout
  - The number of pings answered after the timeout period
  - Late packets as a proportion of the total number
  - Minimum runtime
  - Maximum runtime
  - Average
- Lost
  - The number of lost packets
  - Lost packets as a proportion of the total number
- Last error
  - The last error detected by the tool while attempting to ping the host (e.g. ‘Time Limit Exceeded’ when the host is not reachable).

13.5 Monitoring Internet Connections

LANmonitor can display information about connections to your Internet provider.

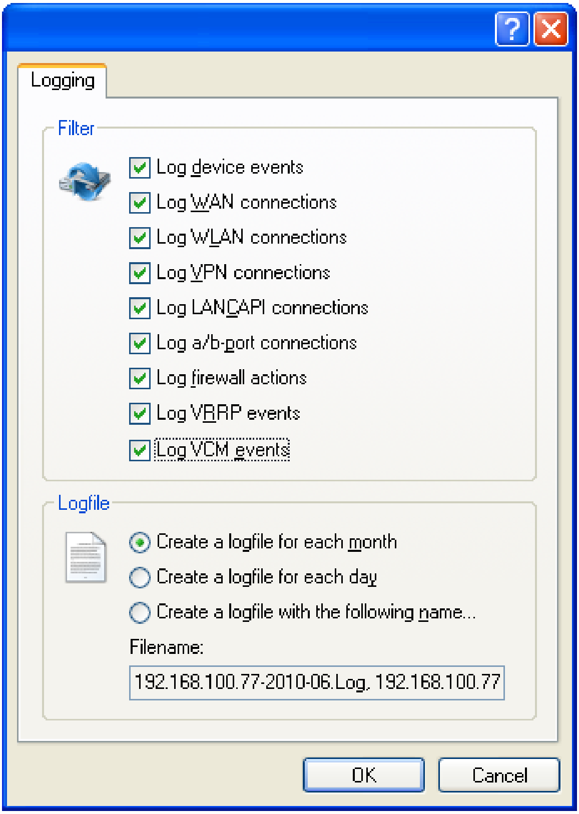
LANmonitor automatically creates a new entry in the device list and initially displays the status of the transfer channels. Start your Web browser and enter the desired web page. LANmonitor shows a connection being established on one channel and the name of the remote site being called. Once the connection is established, a plus sign on the communication channel entry indicates that further information about this channel is available. Click on the plus sign or double-click the appropriate entry to open a tree structure in which you can view various information:



[redacted]
- WAN connections: None
- Wireless LAN
  - WLAN - 1
- Firewall: Active
- System information
  - Device: [redacted]
  - Interfaces
    - WLAN - 1: Atheros AR5414
      - MAC address: 00:02:6f:51:b5:7e
      - Radio band: 2,4 GHz
      - Radio channel: 11
      - Radio-Mode: 802.11g/b (mixed)
      - Transmit power: 15 dBm
      - Noise level: -87 dBm
      - Channel load: 35 %
      - Firmware: Eagle/5[5.3]
    - WLAN - 2: Atheros AR5414

The PPP protocol information lets you determine the IP address assigned to your router by the provider for the duration of the connection, and the addresses transmitted for the DNS and NBNS server.

- To break the connection manually, right-click on the active channel. You may be required to enter a configuration password.
- If you would like a log of the LANmonitor output in file form, select `Device : Device Activities Logging` and select the 'Logging' tab:



Logging

Filter

☑ Log device events
☑ Log WAN connections
☑ Log WLAN connections
☑ Log VPN connections
☑ Log LANCAPI connections
☑ Log a/b-port connections
☑ Log firewall actions
☑ Log VRRP events
☑ Log VCM events

Logfile

● Create a logfile for each month
○ Create a logfile for each day
○ Create a logfile with the following name...

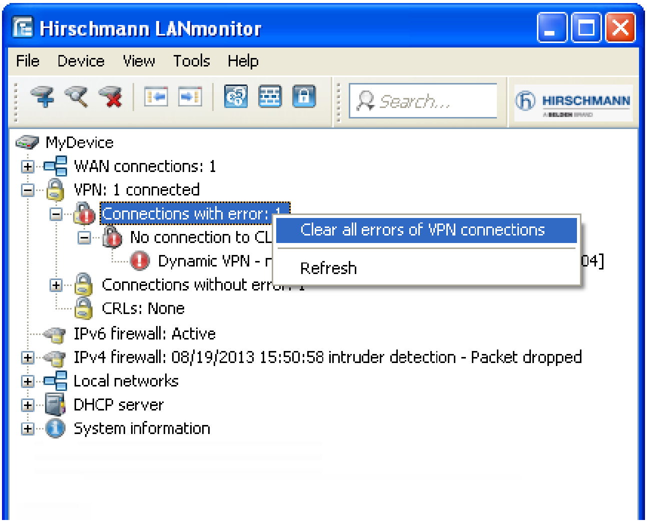
Filename: 192.168.100.77-2010-06.Log, 192.168.100.77

In the above dialog, you can specify the activities to be logged, and how frequently LANmonitor should create a log file: daily, monthly, or on an ongoing basis.

13.6 Delete All VPN Connection Failures

As of HiLCOS version 8.80, LANmonitor gives you the option of deleting all of the VPN connection errors with just one click.

To do this, navigate to the area of LANmonitor for VPN connections, right-click on the entry "Connections with error: x" and select "Clear all VPN connection errors".



Hirschmann LANmonitor

File Device View Tools Help

Search...

HIRSCHMANN

MyDevice
WAN connections: 1
VPN: 1 connected
Connections with error: 1
No connection to CL
Dynamic VPN - r
Connections without error: 1
CRLs: None
IPv6 firewall: Active
IPv4 firewall: 08/19/2013 15:50:58 intruder detection - Packet dropped
Local networks
DHCP server
System information

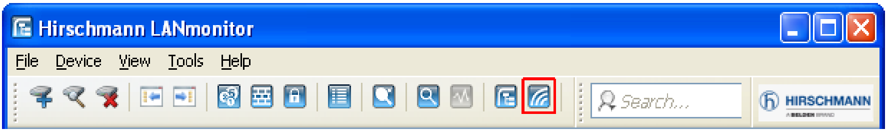
14 Monitoring WLANs with WLANmonitor

WLANmonitor is a component of LANmonitor. You can use WLANmonitor to collect access points into groups. These groups may consist of access points located in buildings, departments, or at individual locations. This helps give you an overview of the entire network for large WLAN infrastructures.

14.1 Starting WLANmonitor

You can open WLANmonitor several ways:

- from LANmonitor using the command `Tools : WLANmonitor`
- from LANmonitor using the WLANmonitor menu button



14.2 Searching for Access Points

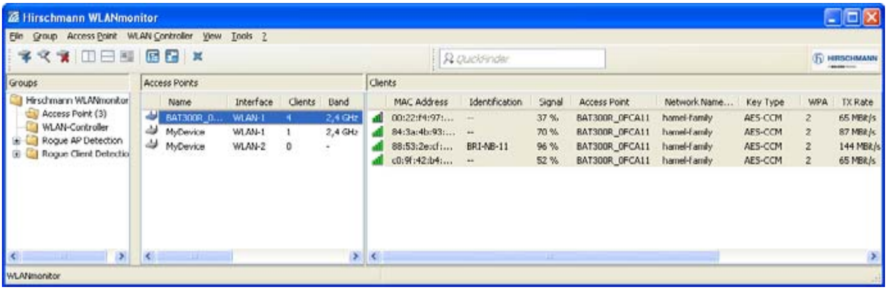
After starting WLANmonitor, you can search for available access points using the `Access Point : Find Access Points` command.

Access Points list:
WLANmonitor lists the access points it discovers in the center of the dialog, along with the following information each access point interface:

- Access point name
- WLAN interface name
- Number of the connected clients
- Frequency band
- Channel
- Transmit power
- Noise level
- Channel load
- IP address of the access point
- Background scan

Clients list:
The right side of the dialog lists the clients that are logged on to each access point, along with the following information for each client:

- Connection Quality: A bar-chart icon indicating signal strength
- MAC address: Hardware address of the WLAN client
- Identification: Name of the client logged in that is entered in the access list or in a RADIUS server.
  LANconfig: `WLAN security : Stations : Stations`
  Telnet: Setup/WLAN/access list
  WEBconfig: `HiLCOS menu tree : Setup : WLAN : Access list`
- Signal: Connection signal strength
- Access point: Name of the access point that the client is logged on to
- Network name (SSID): Identification of the WLAN
- Key type: The type of encryption used for the wireless connection
- WPA version: WPA-1 or WPA-2
- TX rate: Transmission data rate
- RX rate: Reception data rate
- Last error
- IP address of the WLAN client



Access Points

Name	Interface	Clients	Band
BAT300R_0...	WLAN-1	4	2,4 GHz
MyDevice	WLAN-1	1	2,4 GHz
MyDevice	WLAN-2	0	-

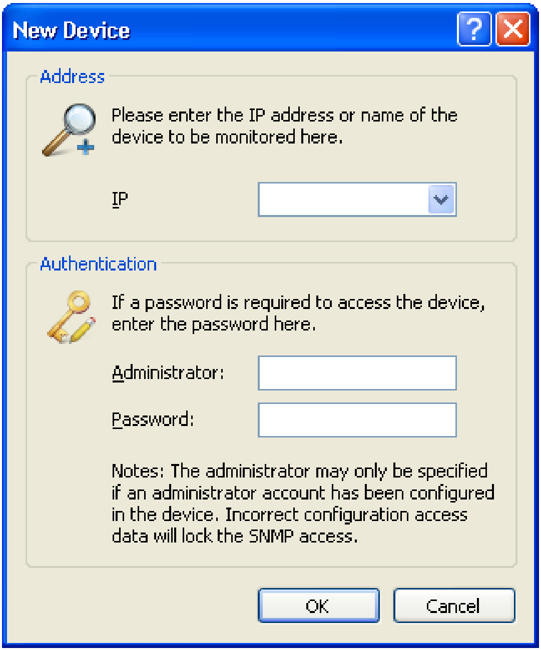
Clients

MAC Address	Identification	Signal	Access Point	Network Name...	Key Type	WPA	TX Rate
00:22:f4:97:...	--	37 %	BAT300R_0FCA11	hamel-family	AES-CCM	2	65 MBit/s
84:3a:4b:93:...	--	70 %	BAT300R_0FCA11	hamel-family	AES-CCM	2	87 MBit/s
88:53:2e:cf:...	BRI-NB-11	96 %	BAT300R_0FCA11	hamel-family	AES-CCM	2	144 MBit/s
c0:9f:42:b4:...	--	52 %	BAT300R_0FCA11	hamel-family	AES-CCM	2	65 MBit/s

14.3 Adding Access Points

If an access point was not recognized automatically, you can manually add it to the list. `Access Point : Add Access Point`.

□ In WLANmonitor, select `Access Point : Add Access Point`.



New Device

Address

Please enter the IP address or name of the device to be monitored here.

IP

Authentication

If a password is required to access the device, enter the password here.

Administrator:

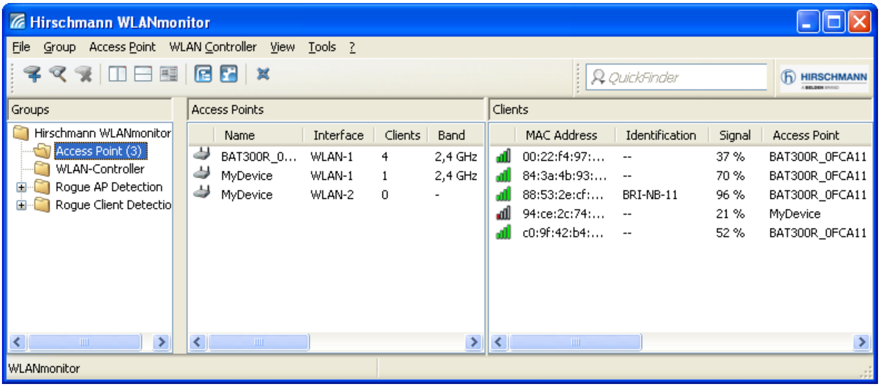
Password:

Notes: The administrator may only be specified if an administrator account has been configured in the device. Incorrect configuration access data will lock the SNMP access.

Use this dialog to enter the IP address or the name of the access point, the administrator name, and the corresponding password.

14.4 Organize Access Points

Use WLANmonitor to organize all available access points independent of their physical location. This helps to maintain an overview of the network and is particularly useful when troubleshooting. Further, WLAN information can be called up according to the groups. You can group your access points according to their departments, locations or applications.
The groups are shown in the left column in WLANmonitor. Starting from the top group “WLANmonitor,” use the command `Group : Add Group` to create new sub-groups and build a structure. Access points found during a search are assigned to the currently selected group in the group tree. Access points that have already been recognized can be dragged and dropped to another group.



Name	Interface	Clients	Band
BAT300R_0...	WLAN-1	4	2,4 GHz
MyDevice	WLAN-1	1	2,4 GHz
MyDevice	WLAN-2	0	-

MAC Address	Identification	Signal	Access Point
00:22:f4:97:...	--	37 %	BAT300R_0FCA11
84:3a:4b:93:...	--	70 %	BAT300R_0FCA11
88:53:2e:cf:...	BRI-NB-11	96 %	BAT300R_0FCA11
94:ce:2c:74:...	--	21 %	MyDevice
c0:9f:42:b4:...	--	52 %	BAT300R_0FCA11

To aid the allocation of access points and clients, you can mark a device by selecting it with the mouse. Any associated devices are also be marked in the list, as follows:

- If an access point is selected in the access point list, all of the clients logged in to this device is also selected in the client list.
- If a client is selected in the client list, the access point that it is associated with it is also selected in the access point list.

14.5 Detecting Rogue Access Points and Rogue Clients with WLANmonitor

WLAN devices that make unauthorized attempts at accessing a WLAN by posing as an access point or client are called rogues.

Rogue clients:
Rogue clients are computers equipped with WLAN adapters that are located within the range of a WLAN and attempt to log on to one of the access points, for example, in order to use the Internet connection or in order to receive access to secured areas on the network.

Rogue Access Points:
An example of a rogue access point is one that a company's employees use to connect to the network without the knowledge or permission of the system administrators. This practice renders a network vulnerable to potential attackers via unsecured WLAN access. Another example is an access point that belongs to third-party networks, but which are within the range of the local WLAN. If such devices use the same service set identity (SSID) and channel as a local access point (for example, by application of default settings), local clients could unintentionally log on to external networks.

Unidentified access points within the range of the local network are not desired. These devices need to be identified to be able to determine whether further measures in securing the local network need to be introduced. Information about the clients within range of your network is automatically stored to an internal table in the OpenBAT wireless router. Once activated, background scanning identifies any neighboring access points, and records them to the scan table. WLANmonitor presents this information visually. The access points and clients found can be categorized in groups such as “known,” “unknown” and “rogue.”

14.5.1 Rogue Access Point Detection

WLANmonitor sorts all of the access points it detects into predefined subgroups, under the folder ‘Rogue AP Detection’. Activate background scanning in the wireless router in order to use rogue access point detection.

Note: Rogue access point detection is active exclusively when background scanning is enabled in the OpenBAT configuration. To enable background scanning, use LANconfig to enter a positive integer value into the ‘Background scan’ property for a WLAN interface in the following location: `Configuration : Wireless LAN : General : Physical WLAN settings : <WLAN interface> : Radio`.

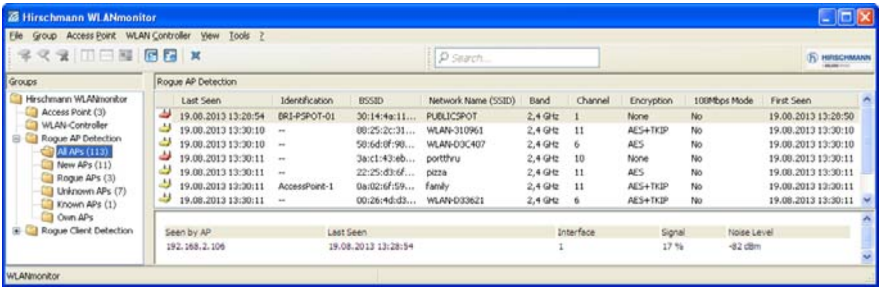
WLANmonitor displays the following under Rogue AP Detection

- Time of first and last detection
- BSSID: The MAC address of the access point for this WLAN network
- Network name
- Type of encryption
- Frequency band
- Radio channel
- Use of 108 Mbps mode

The WLANmonitor uses the following groups for sorting access points:

- All APs: List of all scanned WLAN networks (access points are colored according to their group)
- New APs: New unknown and unconfigured WLAN networks are automatically grouped here (access points are displayed in yellow)
- Rogue APs: WLAN networks identified as rogue and in need of urgent observation (access points are displayed in red)
- Unknown APs: WLAN networks which need to be further analyzed (access points are displayed in gray)
- Known APs: WLAN networks which are not a threat (access points are displayed in gray)
- Own APs: New affiliated WLAN networks from access points monitored by WLANmonitor are automatically grouped here (access points are displayed in green)

The WLANs that have been found can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups (with the exception of the group “All APs”) using the context menu. If a parameter, such as the security settings, is changed on an access point, then it is displayed again as a newly discovered access point.



Rogue AP Detection

Last Seen	Identification	BSSID	Network Name (SSID)	Band	Channel	Encryption	108Mbps Mode	First Seen
19.08.2013 13:28:54	BRI-PSPOT-01	30:14:4a:11...	PUBLICSPOT	2,4 GHz	1	None	No	19.08.2013 13:28:50
19.08.2013 13:30:10	--	08:25:2c:31...	WLAN-310961	2,4 GHz	11	AES+TKIP	No	19.08.2013 13:30:10
19.08.2013 13:30:10	--	58:6d:8f:98...	WLAN-D3C407	2,4 GHz	6	AES	No	19.08.2013 13:30:10
19.08.2013 13:30:11	--	3a:c1:43:eb...	portthru	2,4 GHz	10	None	No	19.08.2013 13:30:11
19.08.2013 13:30:11	--	22:25:d3:6f...	pizza	2,4 GHz	11	AES	No	19.08.2013 13:30:11
19.08.2013 13:30:11	AccessPoint-1	0a:02:6f:59...	family	2,4 GHz	11	AES+TKIP	No	19.08.2013 13:30:11
19.08.2013 13:30:11	--	00:26:4d:d3...	WLAN-D33621	2,4 GHz	6	AES+TKIP	No	19.08.2013 13:30:11

Seen by AP	Last Seen	Interface	Signal	Noise Level
192.168.2.106	19.08.2013 13:28:54	1	17 %	-82 dBm

14.5.2 Rogue Client Detection

WLANmonitor sorts all the clients found into pre-defined subgroups in the “Rogue Client Detection” folder. It is not necessary to configure the OpenBAT device to activate the Rogue Client Detection.

The following information is displayed under Rogue Client Detection:

- Time of first and last detection
- MAC address of the client
- Network name (SSID)

The WLANmonitor uses the following groups for sorting clients:

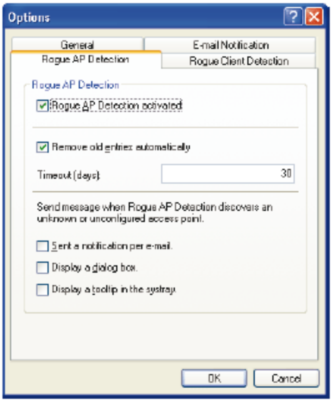
- All clients: List of all found clients (clients are colored according to their group)
- New clients: New unknown clients are automatically grouped here (clients are displayed in yellow)
- Rogue clients: Clients identified as rogue and in need of urgent observation (clients are displayed in red)
- Unknown clients: Clients which need to be further analyzed (clients are displayed in gray)
- Known clients: Clients which are not a threat (clients are displayed in gray)
- Own clients: New affiliated clients associated with access points monitored by WLAN monitor are automatically grouped here (clients are displayed in green)

Clients can be placed into a corresponding group depending on their status. You can set up your own network groups within the individual groups (except for the group “All clients”) using the context menu.

14.5.3 Activating Rogue Access Point and Client Detection

You can activate automatic detection of rogue devices in WLANmonitor:

- For rogue access points:
  `Tools : Options : Rogue AP Detection`
- For rogue clients:
  `Tools : Options : Rogue Client Detection`



Rogue AP Detection

☑ Rogue AP Detection activated

☑ Remove old entries automatically

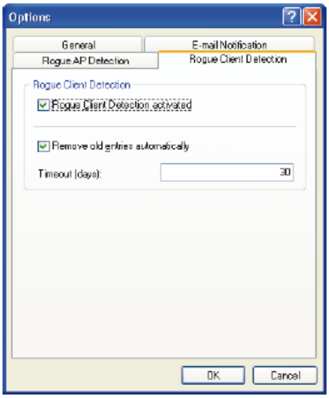
Timeout (days): 30

Send message when Rogue AP Detection discovers an unknown or unconfigured access point.

☐ Sent a notification per e-mail.

☐ Display a dialog box.

☐ Display a tooltip in the systray.



Rogue Client Detection

☑ Rogue Client Detection activated

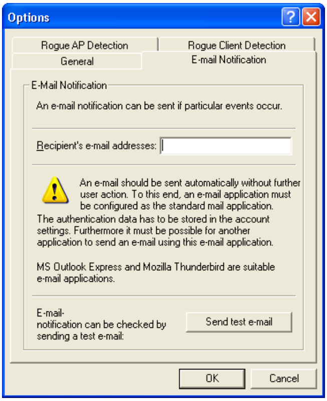
☑ Remove old entries automatically

Timeout (days): 30

14.5.4 Configuring the Alert Function with WLANmonitor

WLANmonitor can inform the administrator automatically via e-mail whenever an unknown or unconfigured access point is discovered. In order to send e-mail alerts, start and configure an e-mail client that supports automatic e-mail transmission on the computer on which WLANmonitor is running.

Enable the e-mail notification function by entering a recipient e-mail address in the `Tools : Options : E-mail Notification` dialog:



An e-mail notification can be sent if particular events occur.

Recipient's e-mail addresses:

An e-mail should be sent automatically without further user action. To this end, an e-mail application must be configured as the standard mail application.
The authentication data has to be stored in the account settings. Furthermore it must be possible for another application to send an e-mail using this e-mail application.

MS Outlook Express and Mozilla Thunderbird are suitable e-mail applications.

E-mail-notification can be checked by sending a test e-mail:

The following features apply to the e-mail function:

- Recipient e-mail addresses
  Enter the e-mail address(es) of the administrators who should be informed in the event of rogue access point detection. Separate multiple e-mail addresses by commas.
- Send a test e-mail
  Some mail clients require a confirmation from the user before sending via third-party applications. Select this option to test your system.

15 Device Diagnostics

Trace outputs may be used to monitor the internal processes in the router during or after configuration. One such trace can be used to display the individual steps involved in negotiating the PPP. Experienced users may interpret these outputs to trace any errors occurring in the establishment of a connection. This helps you determine if a detected event arises from the configuration of your own router or the remote site.

Note: The trace outputs are slightly delayed after the actual event, but are always in the correct sequence. This should be taken into consideration if making precise analyses.

15.1 Starting a Trace in Telnet

Trace output can be started in a Telnet session. Set up a Telnet connection to your device. The command to call up a trace follows this syntax:

```
trace [code] [parameters]
```

The trace command, the code, the parameters and the combination commands are all separated from each other by spaces.

15.1.1 Code Key Overview

The following keys can be used in trace code:

This code...	...combined with the “trace” causes this result...
?	displays a help text
+	switches on a trace output
-	switches off a trace output
#	switches between different trace outputs (toggle)
no code	displays the current status of the trace

15.1.2 Trace Parameters

The trace parameters available depend on the specific OpenBAT device. To call up the list of device parameters available, enter the `trace` command without arguments in the command line.

This parameter ...	...opens the following trace display...
ADSL	ADSL link status
ARP	Address Resolution Protocol
ATM cell	Spoofing at the ATM packet level

This parameter ...	...opens the following trace display...
ATM error	ATM error
Bridge	Information on the wireless LAN bridge
Connact	Messages from the activity protocol
Cron	Cron table
DFS	Trace for Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service Protocol
EAP	Trace for EAP
Error	Connection error messages
Ethernet	Status of Ethernet interface
Firewall	Firewall activities
IAPP	Trace of the inter-access point protocol, displays information about WLAN roaming.
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP Masquerading	Events in the masquerading module
IPX RIP	IPX Routing Information Protocol
IPX router	IPX routing
IPX watchdog	IPX watchdog spoofing
LANAUTH	LAN authentication
LCR	Least-cost router
Load balancer	Load balancing information
Mail client	Email processing with the integrated mail client
NetBIOS	NetBIOS administration
NTP	Timeserver Trace
Display of the first 64 bytes of a package in hexadecimal form	Displays the first 64 bytes of a packet in hexadecimal
PPP	PPP protocol negotiation
RADIUS	RADIUS trace
RIP	IP Routing Information Protocol
SAP	IPX Service Advertising Protocol
Script	Script processing
Serial	Status of serial interface
SMTP client	Email processing with the integrated mail client
SNTP	Simple Network Time Protocol information
Spgtree	Information on the spanning tree protocol
SPX watchdog	SPX watchdog spoofing
Status	Status messages for the connection
USB	Status of USB interface
VLAN	Information concerning virtual networks
VRRP	Information concerning Virtual Router Redundancy Protocol
WLAN	Information concerning wireless networks
XML-Interface-PbSpot	Messages from the Public Spot XML interface

15.1.3 Combination Commands

The following commands can be used to display multiple results:

This combination command...	...opens the following trace display...
Display	status and error outputs
Protocol	ppp and script outputs
TCP-IP	IP-Routing, IP-RIP, ICMP and ARP outputs
IPX-SPX	IPX-Routing, RIP-, SAP-, IPX-Wd., SPX-Wd., and NetBIOS outputs

Any appended parameters are processed from left to right. This means that it is possible to call a parameter and then restrict it.

15.1.4 Trace Filters

Some traces, such as the IP router trace, produce a large quantity of output data. In many instances, the output can become unmanageable. Using trace filters lets you sift out important information. Activate a trace filter by adding the parameter “@“ that induces the following filter description. Trace filters use the following operators:

Operator	Description
(Space):	OR link. The filter applies if one of the operator occurs in the trace output.
+	AND link. The filter applies if the operator occurs in the trace output.
-	NOT link. The filter applies if the operator occurs in the trace output.
"	The output must match the search string exactly.

You can use any character strings as operands, such as the names of remote terminals, protocols or ports. The filter processes these entries based on the rules of the operators used, like the search engines in the internet, for example.

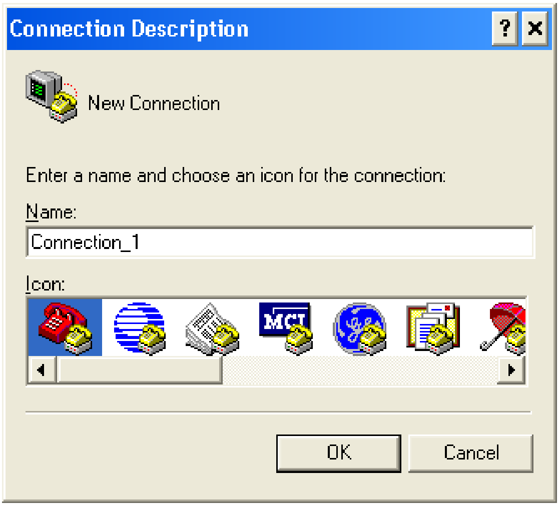
15.1.5 Trace Examples

This code...	...causes the following:
trace	Displays all protocols that can generate outputs during the configuration, and the status of each output (ON or OFF).
trace + protocol display	Switches on the output for all connection protocols together with the status and error messages.
trace - icmp	Switches on all trace outputs with the exception of the ICMP protocol.
trace + ppp	Displays the status of the PPP.
trace # ipx-rt display	Toggles between the trace outputs for the IPX router and the display outputs.
trace + ip-router @ REMOTE SITE-A REMOTE SITE-B	Switches on all trace outputs for IP routers related to remote site A or B.
trace + ip-router @ REMOTE SITE-A REMOTE SITE-B -icmp	Switches on all trace outputs for IP routers related to remote site A or B that do not use ICMP.
trace + ip-router @ REMOTE SITE-A REMOTE SITE-B +ICMP	Switches on all trace outputs for IP routers related to remote site A or B that use ICMP.
trace + ip-router @+TCP +"port: 80"	Switches on all trace outputs from the IP router with TCP/IP and port 80. “port: 80” is in quotes so that the space is recognized as a part of the string.

15.2 Recording Traces with HyperTerminal

Traces can be conveniently recorded under Windows (e.g. as an aid to support), and we recommend you do this as follows:

□ On your PC, start the program HyperTerminal by selecting: `Start : Programs : Accessories : Communications : Hyper Terminal.`



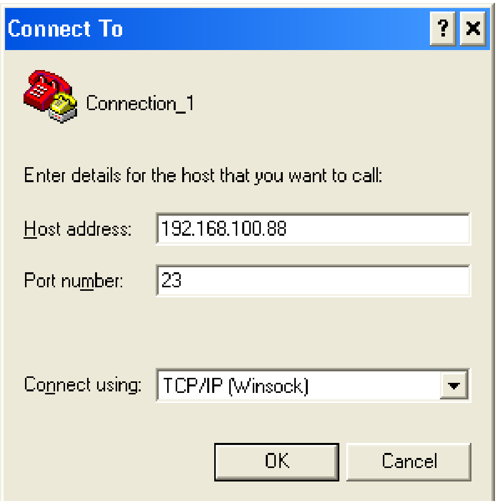
Connection Description

New Connection

Enter a name and choose an icon for the connection:

Name: Connection_1

□ Enter a ‘Name’, select an icon, and click ‘OK’. The ‘Connect To’ dialog opens:



Connection_1

Enter details for the host that you want to call:

Host address: 192.168.100.88

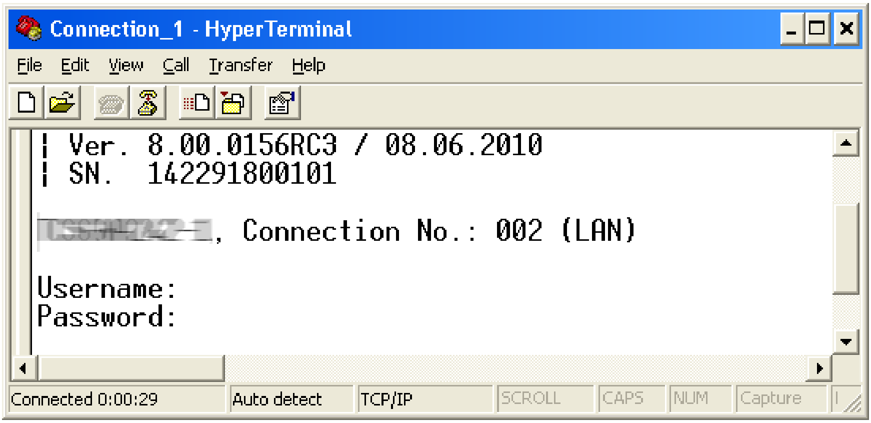
Port number: 23

Connect using: TCP/IP (Winsock)

☐ In the 'Connect To' dialog, enter values for the following fields:

- Connect using: TCP/IP (Winsock)
- Host address: The local/official IP address or the device FQDN.
- Port number: Use the default, port ‘23’.

Click ‘OK’. HyperTerminal displays a request to log in.



```
¦ Ver. 8.00.0156RC3 / 08.06.2010
¦ SN.  142291800101

[redacted], Connection No.: 002 (LAN)

Username:
Password:
```

☐ Enter the ‘Username’ (if any) and click ‘Enter’, then enter the ‘Password’ and again click ‘Enter’.

☐ To record a trace, select `Transfer : Capture Text...`, enter the path to the directory where the text file is to be saved, and click ‘Start’. Now change back to the dialog window and enter the required trace command.

☐ In the Hyper Terminal dialog, enter the required trace command at the command line.

☐ To end the trace, select `Transfer : Capture Text : Stop`.

15.3 Tracing with LANmonitor

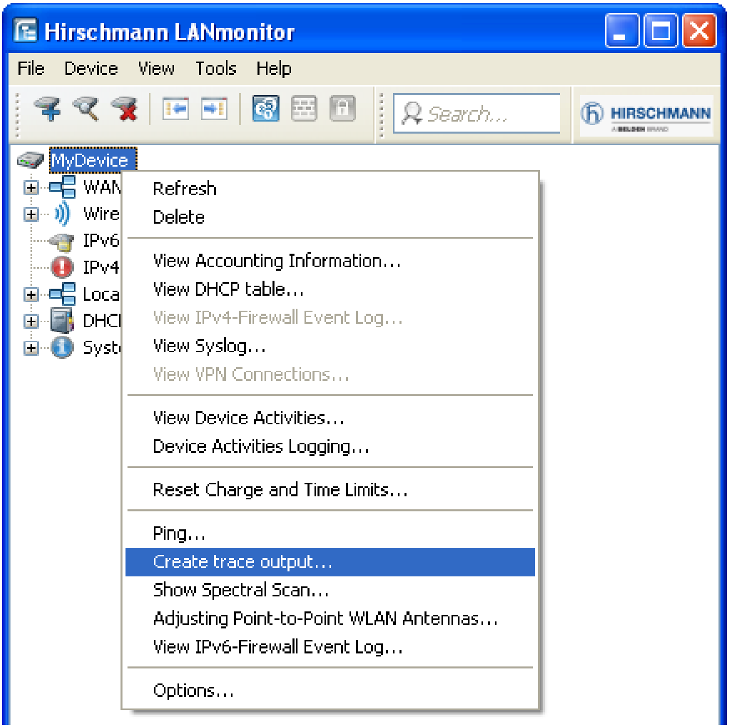
The trace function in LANmonitor is more robust than the standard trace functions available via Telnet, and offers greater convenience in the generation and analysis of traces.

For example, a trace configuration that triggers desired trace commands can be stored to a configuration file. An experienced service technician can program a trace configuration and deliver it to a less experienced operator who then can execute specialized trace requests for a device. Trace results can be stored in a file and returned to the technician for analysis.

Telnet-access to the device must be enabled to carry out trace requests with LANmonitor. When starting the trace dialog, LANmonitor first attempts to establish an SSL-encrypted Telnet connection to the device. If the device does not support SSL connections, LANmonitor automatically switches to unencrypted Telnet.

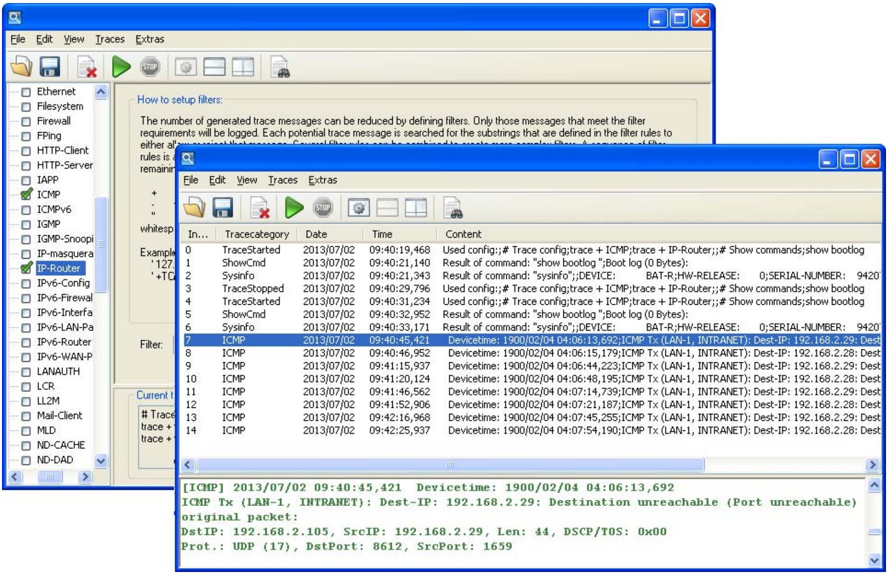
To open the “Traces” dialog for a specific OpenBAT device:

☐ Right-click the device entry in LANmonitor and select “Traces” in the context menu:


Hirschmann LANmonitor
File Device View Tools Help
Search...
HIRSCHMANN
MyDevice
WAN
Wire
IPv6
IPv4
Loca
DHCI
Syst
Refresh
Delete
View Accounting Information...
View DHCP table...
View IPv4-Firewall Event Log...
View Syslog...
View VPN Connections...
View Device Activities...
Device Activities Logging...
Reset Charge and Time Limits...
Ping...
Create trace output...
Show Spectral Scan...
Adjusting Point-to-Point WLAN Antennas...
View IPv6-Firewall Event Log...
Options...

▶ If SNMP access to the device is password-protected, enter the access data—name and password—for an administrator with trace rights in order to proceed with the trace.

The ‘Traces’ dialog presents two different appearances: configuration mode (left, below) and output display mode (right, below):



The number of generated trace messages can be reduced by defining filters. Only those messages that meet the filter requirements will be logged. Each potential trace message is searched for the substrings that are defined in the filter rules to

```
In...  Tracecategory  Date        Time          Content
0      TraceStarted   2013/07/02  09:40:19,468  Used config:;# Trace config;trace + ICMP;trace + IP-Router;;# Show commands;show bootlog
1      ShowCmd        2013/07/02  09:40:21,140  Result of command: "show bootlog ";Boot log (0 Bytes):
2      Sysinfo        2013/07/02  09:40:21,343  Result of command: "sysinfo";;DEVICE:       BAT-R;HW-RELEASE:     0;SERIAL-NUMBER:   9420
3      TraceStopped   2013/07/02  09:40:29,796  Used config:;# Trace config;trace + ICMP;trace + IP-Router;;# Show commands;show bootlog
4      TraceStarted   2013/07/02  09:40:31,234  Used config:;# Trace config;trace + ICMP;trace + IP-Router;;# Show commands;show bootlog
5      ShowCmd        2013/07/02  09:40:32,952  Result of command: "show bootlog ";Boot log (0 Bytes):
6      Sysinfo        2013/07/02  09:40:33,171  Result of command: "sysinfo";;DEVICE:       BAT-R;HW-RELEASE:     0;SERIAL-NUMBER:   9420
7      ICMP           2013/07/02  09:40:45,421   Devicetime: 1900/02/04 04:06:13,692;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.29: Dest
8      ICMP           2013/07/02  09:40:46,952   Devicetime: 1900/02/04 04:06:15,179;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.28: Dest
9      ICMP           2013/07/02  09:41:15,937   Devicetime: 1900/02/04 04:06:44,223;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.29: Dest
10     ICMP           2013/07/02  09:41:20,124   Devicetime: 1900/02/04 04:06:48,195;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.28: Dest
11     ICMP           2013/07/02  09:41:46,562   Devicetime: 1900/02/04 04:07:14,739;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.29: Dest
12     ICMP           2013/07/02  09:41:52,906   Devicetime: 1900/02/04 04:07:21,187;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.28: Dest
13     ICMP           2013/07/02  09:42:16,968   Devicetime: 1900/02/04 04:07:45,255;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.29: Dest
14     ICMP           2013/07/02  09:42:25,937   Devicetime: 1900/02/04 04:07:54,190;ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.28: Dest
```

```
[ICMP] 2013/07/02 09:40:45,421  Devicetime: 1900/02/04 04:06:13,692
ICMP Tx (LAN-1, INTRANET): Dest-IP: 192.168.2.29: Destination unreachable (Port unreachable)
original packet:
DstIP: 192.168.2.105, SrcIP: 192.168.2.29, Len: 44, DSCP/TOS: 0x00
Prot.: UDP (17), DstPort: 8612, SrcPort: 1659
```

The LANmonitor ‘Traces’ dialog presents the following command buttons for operating traces:

Icon	Description
📂	Opens a pre-defined configuration for the trace command.
💾	Saves the current trace configuration.
📥	Opens a file with trace results for viewing in the ‘Traces’ dialog.
📤	Saves the current trace results to a file.
📄	Clears the current display or trace results.
▶	Starts outputting the trace results as produced by the current configuration and automatically switches the ‘Traces’ dialog interface to trace output display mode.
🟥	Stops the output of trace results.

Icon	Description
📋	Switches the ‘Traces’ dialog interface to configuration mode.
▭	Switches he ‘Traces’ dialog interface to trace output display mode.

15.3.1 Creating Traces with the Trace Configuration Wizard

The trace settings can be configured very easily using the Trace Configuration Wizard. To use the wizard, follow these steps:

□ With the ‘Traces’ dialog open for a selected device, select: `<Device Name> : Guided configuration`.

□ Click the ‘Start wizard’ button to open the wizard, then follow the steps presented in the wizard.

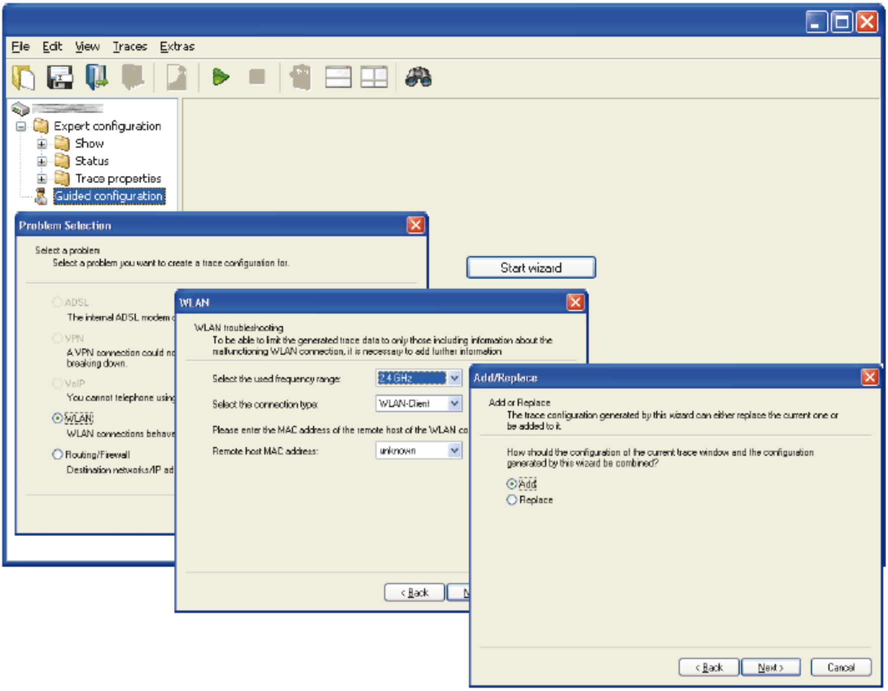
Trace functions (e.g. WLAN) can be selected in the wizard dialogs, and the trace can be restricted as needed (for example, to a particular remote host).

The last step in the wizard is to indicate how the new trace configuration, created by the wizard, should be saved. Select either:

▶ Add, to combine the new configuration with the current trace configuration displayed in the ‘Traces’ dialog.

▶ Replace, to save only the new configuration created by the wizard, and deleting the previous trace configuration.

Note: Except for the bootleg trace (which is included automatically), all previous trace settings are deleted when the trace configuration is replaced. Save the previous trace configuration for later use before running the trace configuration wizard.



Problem Selection

Select a problem
Select a problem you want to create a trace configuration for.

○ ADSL
The internal ADSL modem

○ VPN
A VPN connection could no
breaking down.

○ VoIP
You cannot telephone using

● WLAN
WLAN connections behave

○ Routing/Firewall
Destination networks/IP ad

WLAN

WLAN troubleshooting
To be able to limit the generated trace data to only those including information about the malfunctioning WLAN connection, it is necessary to add further information

Select the used frequency range: 2.4 GHz

Select the connection type: WLAN-Client

Please enter the MAC address of the remote host of the WLAN co

Remote host MAC address: unknown

Add/Replace

Add or Replace
The trace configuration generated by this wizard can either replace the current one or be added to it.

How should the configuration of the current trace window and the configuration generated by this wizard be combined?

● Add
○ Replace

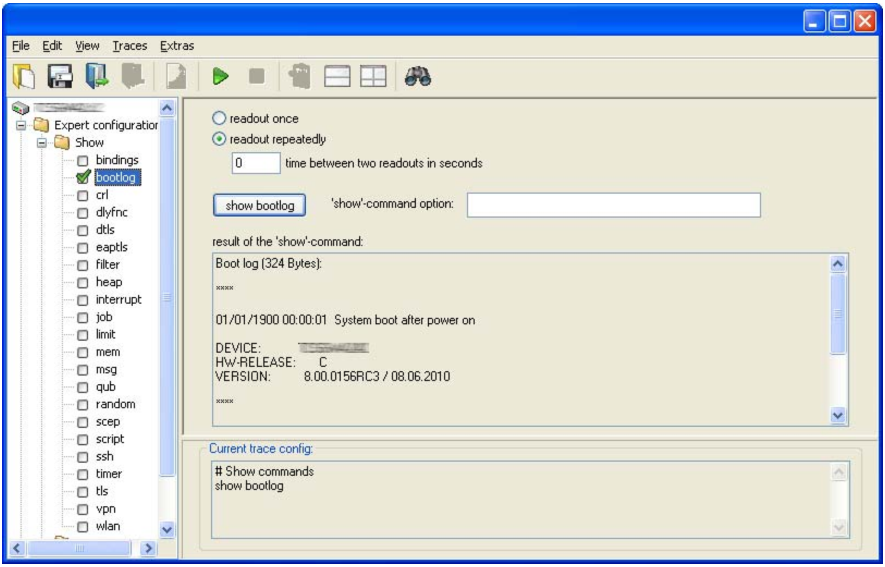
15.3.2 Manually Creating Trace Configurations

In addition to creating trace configurations with the wizard, you can also manually create trace configurations in the 'Traces' dialog, as follows:

- ☐ With the 'Traces' dialog open for a selected device, select: `<Device Name> : Expert configuration`.
- ☐ Enter trace settings in the `Show`, `Status`, and `Trace properties` folders. These folders and their contents are described, below.

Show folder settings

Use the contents of the ‘Show’ folder to retrieve device data that would ordinarily be obtained using the `Show` command from a command line interface (e.g. Telnet). You can either manually execute the `Show` command and immediately display selected device data, or you can add a `Show` command to the Trace configuration that will later be executed and generate the Trace dump.



○ readout once

● readout repeatedly

0 time between two readouts in seconds

'show'-command option:

result of the 'show'-command:

```
Boot log (324 Bytes):

****

01/01/1900 00:00:01  System boot after power on

DEVICE:        [redacted]
HW-RELEASE:     C
VERSION:        8.00.0156RC3 / 08.06.2010

****
```

Current trace config:

```
# Show commands
show bootlog
```

▶ Immediately display selected data:
You can manually display current values for selected device data. To do this, follow these steps:

☐ Open the ‘Show’ folder and highlight one of the available data selections for the device. The ‘show’ button displays the data selection.

☐ Depending upon the selection, you may elect to—or may be required to—enter additional parameters in the input box labeled: ‘show-command option’.

☐ Click the ‘show’ button. Device data of the selected type is displayed in the ‘result’ area.

▶ Add a ‘Show’ command to the Trace dump:
To add a command to the Trace dump, follow these steps:

☐ Open the ‘Show’ folder and place a check mark in the check-box to the left one of the available data selections for the device. This enables the ‘readout’ selections for the entry.

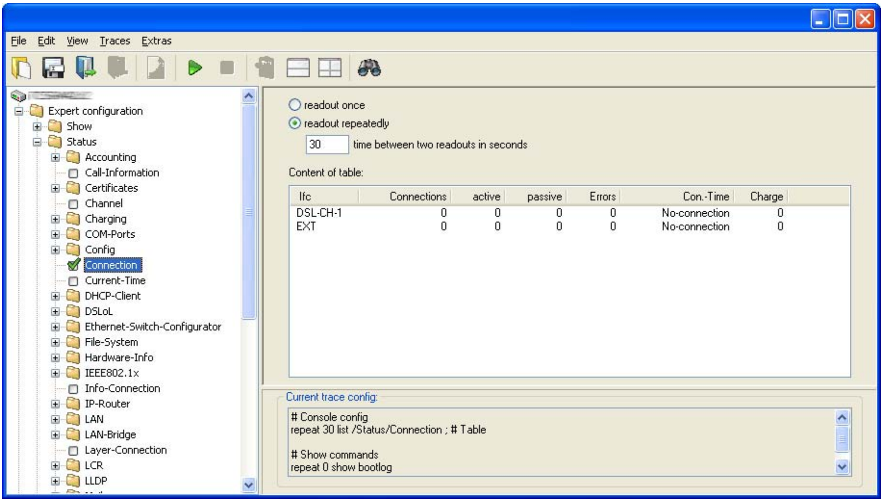
☐ Specify the readout frequency, i.e., how often the selected data will be read as part of the Trace dump:
–readout once

–readout repeatedly (and type in the time between readouts)

The selected entry is added to the Trace configuration, and appears as a line added to the ‘Current trace config’ area.

Status folder settings

You can access comprehensive status information and statistics for a device in the ‘Status’ folder of the ‘Traces’ dialog. Depending on your selection, the information accessed will be in the form of either a discrete value, or a table of values.



○ readout once
● readout repeatedly
30 time between two readouts in seconds

Content of table:

Ifc	Connections	active	passive	Errors	Con.-Time	Charge
DSL-CH-1	0	0	0	0	No-connection	0
EXT	0	0	0	0	No-connection	0

Current trace config:

```
# Console config
repeat 30 list /Status/Connection ; # Table

# Show commands
repeat 0 show bootlog
```

To display the current contents of the table or value, click the name of a status entry in the left-hand area of the trace dialogue. To accept the dump of the Status entry into the trace data, click the appropriate checkbox to the left of the entry name. For every Status entry enabled, a setting defines whether it is read out once only on starting the trace or whether it is read out at regular intervals (set in seconds).

□ Open the ‘Status’ folder and select one of the available status entries for the device. The item value or the table values are displayed.

□ To add the item as a Status entry in the Trace dump, place a check mark in the check-box next to the item. This enables the ‘readout’ selections for the Status entry.

□ Specify the readout frequency, i.e., how often the selected status information will be read as part of the Trace dump:
- readout once
- readout repeatedly (and type in the time between readouts)

The selected entry is added to the Trace configuration, and appears as a line added to the ‘Current trace config’ area.

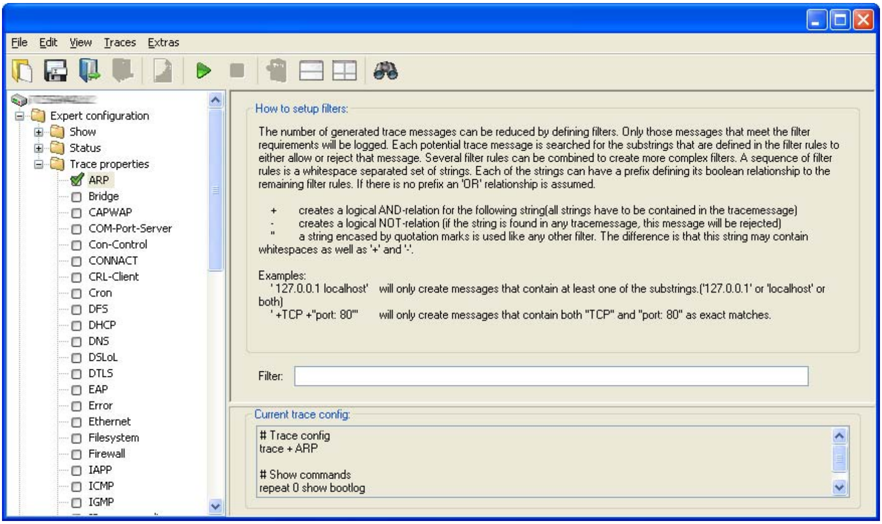
Note: This device Status information also can be accessed from the command line (Telnet) or via WEBconfig.

Trace properties folder settings

The traces to be dumped for the current device can be enabled in the trace settings area. To include the dump of the trace into the trace data:

□ Open the ‘Status’ folder and select one of the available trace entries for the device. The ‘Filter’ field for the entry is enabled.

A filter can be entered for every trace. For example, if you want to display only the IP traces of a particular workstation, enter the appropriate IP address as a filter of the IP router trace.



How to setup filters:

The number of generated trace messages can be reduced by defining filters. Only those messages that meet the filter requirements will be logged. Each potential trace message is searched for the substrings that are defined in the filter rules to either allow or reject that message. Several filter rules can be combined to create more complex filters. A sequence of filter rules is a whitespace separated set of strings. Each of the strings can have a prefix defining its boolean relationship to the remaining filter rules. If there is no prefix an 'OR' relationship is assumed.

+ creates a logical AND-relation for the following string(all strings have to be contained in the tracemessage)
- creates a logical NOT-relation (if the string is found in any tracemessage, this message will be rejected)
" a string encased by quotation marks is used like any other filter. The difference is that this string may contain whitespaces as well as '+' and '-'.

Examples:
' 127.0.0.1 localhost' will only create messages that contain at least one of the substrings.('127.0.0.1' or 'localhost' or both)
' +TCP +"port: 80"' will only create messages that contain both "TCP" and "port: 80" as exact matches.

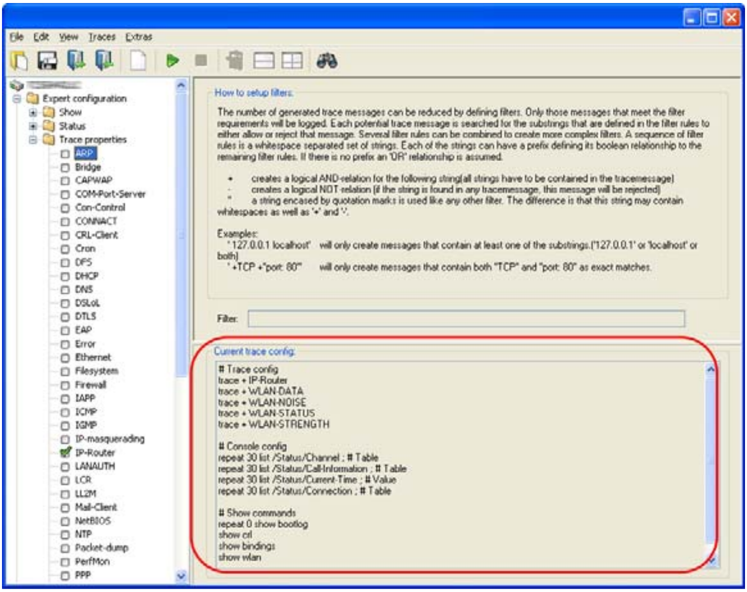
Filter:

Current trace config:

```
# Trace config
trace + ARP

# Show commands
repeat 0 show bootlog
```

15.3.3 Displaying Trace Data

The entire trace configuration is shown in the lower area of the dialog where all active Trace properties, Status and Show entries are listed with the respective filters and parameters.



How to setup filters:

The number of generated trace messages can be reduced by defining filters. Only those messages that meet the filter requirements will be logged. Each potential trace message is searched for the substrings that are defined in the filter rules to either allow or reject that message. Several filter rules can be combined to create more complex filters. A sequence of filter rules is a whitespace separated set of strings. Each of the strings can have a prefix defining its boolean relationship to the remaining filter rules. If there is no prefix an 'OR' relationship is assumed.

+ creates a logical AND-relation for the following string(all strings have to be contained in the tracemessage)
- creates a logical NOT-relation (if the string is found in any tracemessage, this message will be rejected)
" a string encased by quotation marks is used like any other filter. The difference is that this string may contain whitespaces as well as '+' and '-'.

Examples:
'127.0.0.1 localhost' will only create messages that contain at least one of the substrings.('127.0.0.1' or 'localhost' or both)
' +TCP +"port: 80"' will only create messages that contain both "TCP" and "port: 80" as exact matches.

Current trace config:

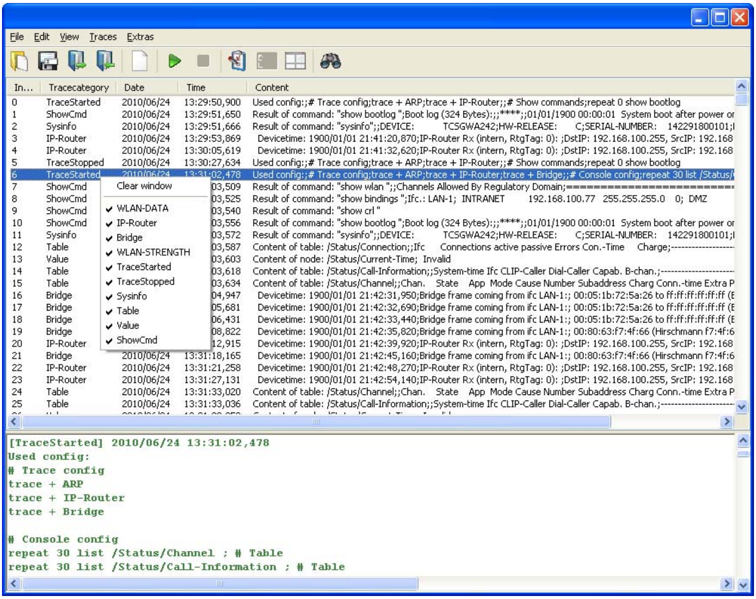
```
# Trace config
trace + IP-Router
trace + WLAN-DATA
trace + WLAN-NOISE
trace + WLAN-STATUS
trace + WLAN-STRENGTH

# Console config
repeat 30 list /Status/Channel ; # Table
repeat 30 list /Status/Call-Information ; # Table
repeat 30 list /Status/Current-Time ; # Value
repeat 30 list /Status/Connection ; # Table

# Show commands
repeat 0 show bootlog
show crl
show bindings
show wlan
```

To start the dump of the trace data, use the `Traces : Start tracing` menu command, or click the ‘Start tracing’ button (with the green arrowhead). The ‘Traces’ dialog presents the trace output display:

- Trace events are displayed in the top part of the dialog.
- Results of a selected event are displayed in the bottom part of the dialog.

You have the option of editing the trace results displayed in the upper section of the dialog using the context menu. Carry out the following steps:

- ☐ Click the right mouse button in the top of the dialog, to open the context menu.
- ☐ Select/de-select the traces to be displayed, or select ‘Clear window’ to empty the list of trace events.



In...	Tracecategory	Date	Time	Content
0	TraceStarted	2010/06/24	13:29:50,900	Used config:;# Trace config;trace + ARP;trace + IP-Router;;# Show commands;repeat 0 show bootlog
1	ShowCmd	2010/06/24	13:29:51,650	Result of command: "show bootlog ";Boot log (324 Bytes):;;****;;01/01/1900 00:00:01 System boot after power or
2	Sysinfo	2010/06/24	13:29:51,666	Result of command: "sysinfo";;DEVICE: TCSGWA242;HW-RELEASE: C;SERIAL-NUMBER: 142291800101;I
3	IP-Router	2010/06/24	13:29:53,869	Devicetime: 1900/01/01 21:41:20,870;IP-Router Rx (intern, RtgTag: 0): ;DstIP: 192.168.100.255, SrcIP: 192.168
4	IP-Router	2010/06/24	13:30:05,619	Devicetime: 1900/01/01 21:41:32,620;IP-Router Rx (intern, RtgTag: 0): ;DstIP: 192.168.100.255, SrcIP: 192.168
5	TraceStopped	2010/06/24	13:30:27,634	Used config:;# Trace config;trace + ARP;trace + IP-Router;;# Show commands;repeat 0 show bootlog
6	TraceStarted	2010/06/24	13:31:02,478	Used config:;# Trace config;trace + ARP;trace + IP-Router;trace + Bridge;;# Console config;repeat 30 list /Status/
7	ShowCmd		03,509	Result of command: "show wlan ";;Channels Allowed By Regulatory Domain;=========================
8	ShowCmd		03,525	Result of command: "show bindings ";Ifc.: LAN-1; INTRANET 192.168.100.77 255.255.255.0 0; DMZ
9	ShowCmd		03,540	Result of command: "show crl "
10	ShowCmd		03,556	Result of command: "show bootlog ";Boot log (324 Bytes):;;****;;01/01/1900 00:00:01 System boot after power or
11	Sysinfo		03,572	Result of command: "sysinfo";;DEVICE: TCSGWA242;HW-RELEASE: C;SERIAL-NUMBER: 142291800101;I
12	Table		03,587	Content of table: /Status/Connection;;Ifc Connections active passive Errors Con.-Time Charge;------------------
13	Value		03,603	Content of node: /Status/Current-Time; Invalid
14	Table		03,618	Content of table: /Status/Call-Information;;System-time Ifc CLIP-Caller Dial-Caller Capab. B-chan.;--------------------
15	Table		03,634	Content of table: /Status/Channel;;Chan. State App Mode Cause Number Subaddress Charg Conn.-time Extra P
16	Bridge		04,947	Devicetime: 1900/01/01 21:42:31,950;Bridge frame coming from ifc LAN-1:; 00:05:1b:72:5a:26 to ff:ff:ff:ff:ff:ff (E
17	Bridge		05,681	Devicetime: 1900/01/01 21:42:32,690;Bridge frame coming from ifc LAN-1:; 00:05:1b:72:5a:26 to ff:ff:ff:ff:ff:ff (E
18	Bridge		06,431	Devicetime: 1900/01/01 21:42:33,440;Bridge frame coming from ifc LAN-1:; 00:05:1b:72:5a:26 to ff:ff:ff:ff:ff:ff (E
19	Bridge		08,822	Devicetime: 1900/01/01 21:42:35,820;Bridge frame coming from ifc LAN-1:; 00:80:63:f7:4f:66 (Hirschmann f7:4f:6
20	IP-Router		12,915	Devicetime: 1900/01/01 21:42:39,920;IP-Router Rx (intern, RtgTag: 0): ;DstIP: 192.168.100.255, SrcIP: 192.168
21	Bridge	2010/06/24	13:31:18,165	Devicetime: 1900/01/01 21:42:45,160;Bridge frame coming from ifc LAN-1:; 00:80:63:f7:4f:66 (Hirschmann f7:4f:6
22	IP-Router	2010/06/24	13:31:21,258	Devicetime: 1900/01/01 21:42:48,270;IP-Router Rx (intern, RtgTag: 0): ;DstIP: 192.168.100.255, SrcIP: 192.168
23	IP-Router	2010/06/24	13:31:27,131	Devicetime: 1900/01/01 21:42:54,140;IP-Router Rx (intern, RtgTag: 0): ;DstIP: 192.168.100.255, SrcIP: 192.168
24	Table	2010/06/24	13:31:33,020	Content of table: /Status/Channel;;Chan. State App Mode Cause Number Subaddress Charg Conn.-time Extra P
25	Table	2010/06/24	13:31:33,036	Content of table: /Status/Call-Information;;System-time Ifc CLIP-Caller Dial-Caller Capab. B-chan.;--------------------

```
[TraceStarted] 2010/06/24 13:31:02,478
Used config:
# Trace config
trace + ARP
trace + IP-Router
trace + Bridge

# Console config
repeat 30 list /Status/Channel ; # Table
repeat 30 list /Status/Call-Information ; # Table
```

Note: Trace data is collected while the trace dump is enabled, and is periodically written to a back-up file. Refer to ‘Back Up Settings for Traces’ (see page 236).

15.3.4 Backing Up and Restoring Trace Configurations

The entire configuration of the trace dump can be written to a storage medium for later re-use or for transfer to another user.

To back up a trace configuration:

□ In the ‘Traces’ dialog, select `File : Save trace config`, then navigate to the location where you want to save the trace configuration.

To restore a trace configuration:

□ In the ‘Traces’ dialog, select `File : Load trace config`, then navigate to the location where the saved trace configuration is stored.

15.3.5 Saving and Restoring Trace Data

For later editing, or for transfer to another user, the actual trace data can be written to a storage medium and later re-opened.

To back up trace data:

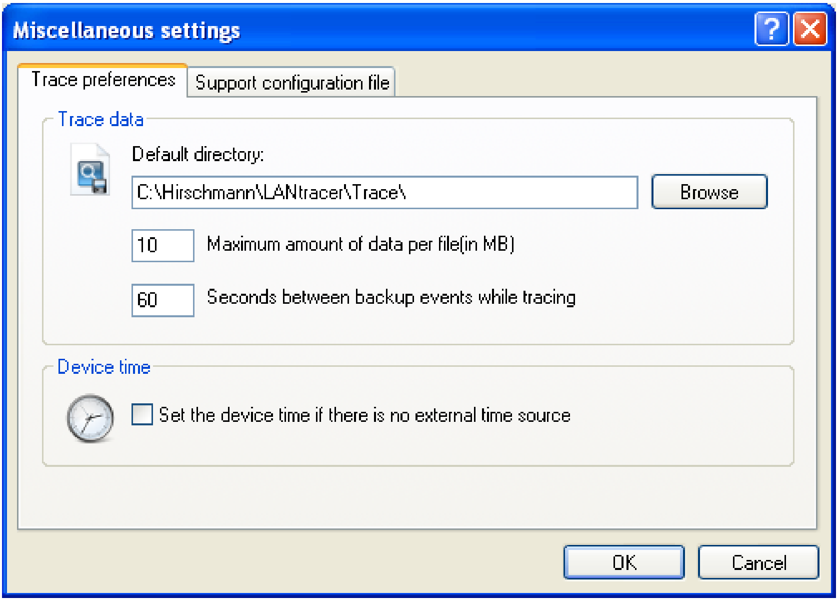
□ In the ‘Traces’ dialog, select:
`File : Save trace data/support configuration`, then navigate to the location where you want to save the trace data.

To restore trace data:

□ In the ‘Traces’ dialog, select `File : Load trace data`, then navigate to the location where the saved trace data is stored.

15.3.6 Back-Up Settings for Traces

When starting a trace in the ‘Traces’ dialog, a back-up file with the current trace data is automatically saved. The settings for the trace back-up can be configured at the following location:
`Extras : Miscellaneous settings : Trace preferences`.



Trace data

Default directory:

C:\Hirschmann\LANtracer\Trace\

10 Maximum amount of data per file(in MB)

60 Seconds between backup events while tracing

Device time

☐ Set the device time if there is no external time source

The following settings can be configured for trace back-up:

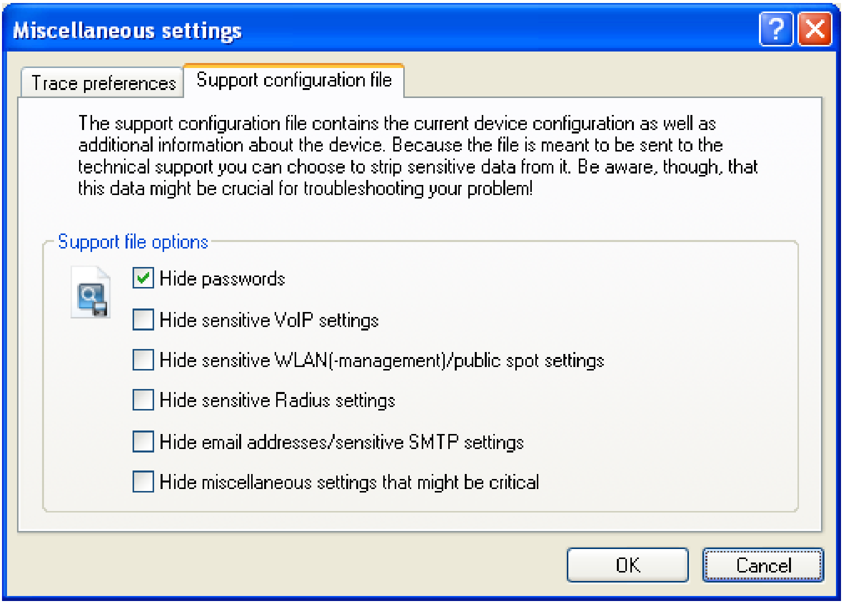
- Default directory for trace data
- Threshold in megabytes after which a new trace data file will be created: This sets the maximum size of the back-up file.
- Seconds after which newly generated data of an active trace is saved as back-up: This is the save interval for the back-up file.
- Set the current time on devices with an invalid or manually set time: Because some traced devices do not have valid time information, this setting applies workstation time as the device time.

15.3.7 Saving Support File

A support file enables all information pertaining to device support to be easily written to one file. This data can include:

- Trace data as configured in the current settings
- Current device configuration
- Bootlog
- Sysinfo

When saving the device configuration, you can hide security-related information of no relevance. This can be configured in the ‘Traces’ dialog at `Extras : Miscellaneous settings : Support configuration file`



Miscellaneous settings

Trace preferences | Support configuration file

The support configuration file contains the current device configuration as well as additional information about the device. Because the file is meant to be sent to the technical support you can choose to strip sensitive data from it. Be aware, though, that this data might be crucial for troubleshooting your problem!

Support file options

☑ Hide passwords

□ Hide sensitive VoIP settings

□ Hide sensitive WLAN(-management)/public spot settings

□ Hide sensitive Radius settings

□ Hide email addresses/sensitive SMTP settings

□ Hide miscellaneous settings that might be critical

15.4 Performance Monitoring with LANmonitor

LANmonitor logs various parameters in the devices and displays these graphically:

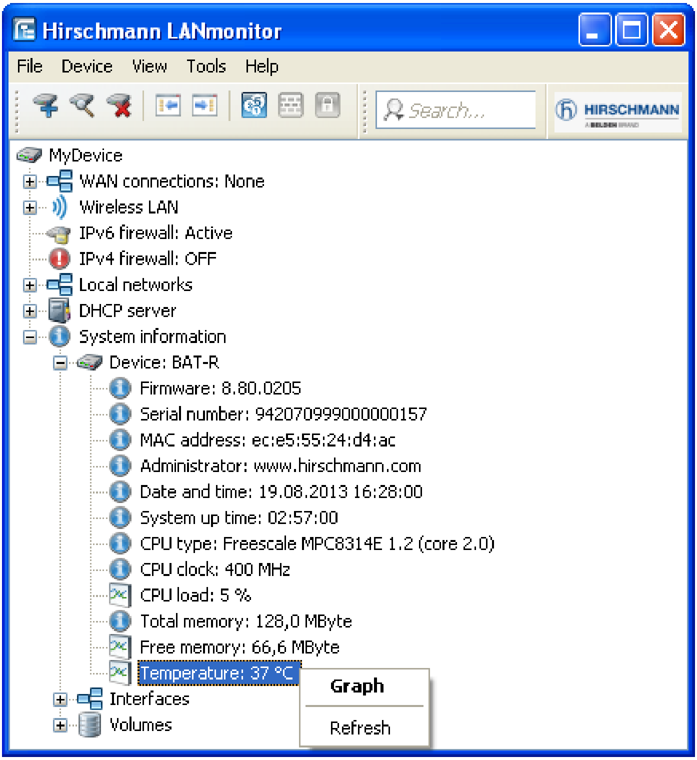
- ▶ Transmit and receive rates for WAN connections
- ▶ Transmit and receive rates for point-to-point connections
- ▶ Signal reception strength for point-to-point connections
- ▶ Link signal strength for point-to-point connections
- ▶ Throughput for point-to-point connections
- ▶ CPU load
- ▶ Free memory
- ▶ Temperature (not available on all models)

LANmonitor displays the current values directly in the corresponding groups.

To display a graphical log of monitored data:

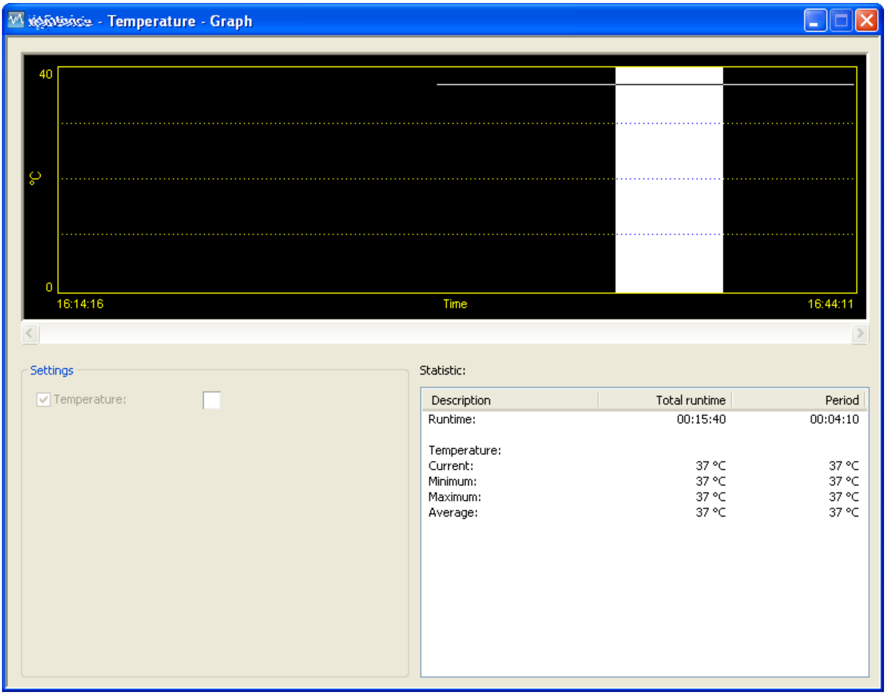
☐ In LANmonitor, select a parameter that can be displayed graphically, and click the right mouse button.

☐ Select `Graph` in the context menu.



MyDevice
WAN connections: None
Wireless LAN
IPv6 firewall: Active
IPv4 firewall: OFF
Local networks
DHCP server
System information
Device: BAT-R
Firmware: 8.80.0205
Serial number: 942070999000000157
MAC address: ec:e5:55:24:d4:ac
Administrator: www.hirschmann.com
Date and time: 19.08.2013 16:28:00
System up time: 02:57:00
CPU type: Freescale MPC8314E 1.2 (core 2.0)
CPU clock: 400 MHz
CPU load: 5 %
Total memory: 128,0 MByte
Free memory: 66,6 MByte
Temperature: 37 °C
Interfaces
Volumes

A new graph window opens that displays the selected parameter value over time:



Settings

☑ Temperature: □

Statistic:

Description	Total runtime	Period
Runtime:	00:15:40	00:04:10
Temperature:		
Current:	37 °C	37 °C
Minimum:	37 °C	37 °C
Maximum:	37 °C	37 °C
Average:	37 °C	37 °C

You can hold down the left mouse key and drag it over a part of the graph to mark that time period. The statistical values associated with that time period are displayed separately.

Note: These graphically displayed values are deleted when the window is closed. For monitoring over a longer period, leave the window open.

15.5 SYSLOG

The SYSLOG protocol records the activities of a OpenBAT device. You use this function to log the entire progress of all the activities in the device.

15.5.1 Accessing SYSLOG Data

The information captured in the SYSLOG log can be handled in different ways:

■ Central Collection Point

You have the option of sending the SYSLOG messages to a central collection point, known as the SYSLOG client or daemon. This option is useful if, for example, you have to record messages from a large number of devices.

▶ Logging under UNIX/Linux:
Under UNIX/Linux the logging is usually performed by the SYSLOG daemon, which is usually set up as standard. The daemon either reports directly via the console or writes the log in a corresponding SYSLOG file. The `/etc/syslog.conf` file specifies which facilities are to be written in which log file.

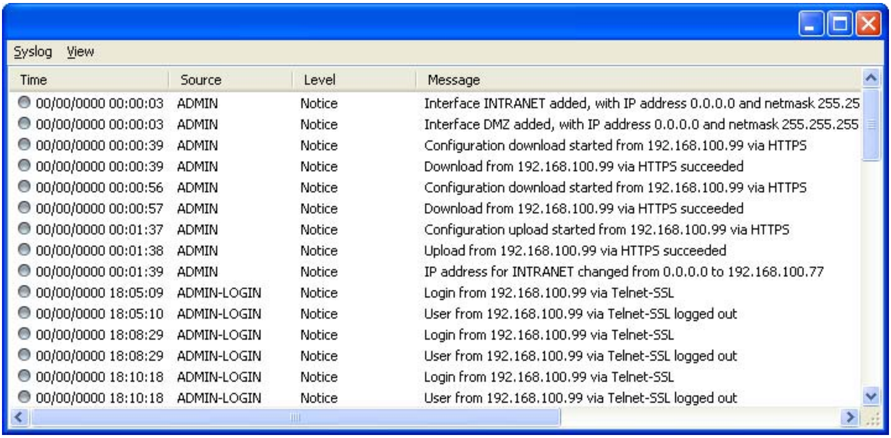
Note: In the configuration of the daemon, check whether it explicitly monitors network connections.

- Logging under Windows:
  Windows does not provide a corresponding system function. You require special software that fulfills the function of a SYSLOG daemon.
- Logging in the device memory:
  You have the option of configuring every OpenBAT device to manage a SYSLOG file in its memory.

Accessing SYSLOG in Device Memory

The most recent SYSLOG messages are stored in the device's RAM. Depending on the memory size, this can vary from 100 to 2048 SYSLOG messages. These internal SYSLOGs can be viewed using the following tools:

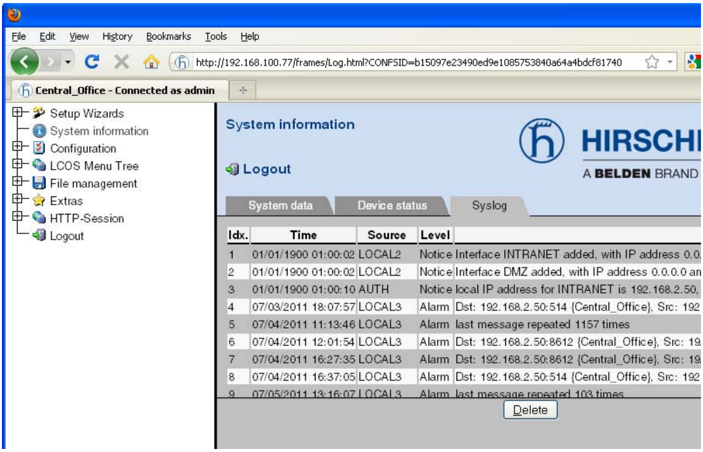
- Telnet, in the device statistics using the command line.
- LANmonitor:
  You can access a snapshot of the current SYSLOG file via LANmonitor: highlight a device, then select `Device : View Syslog`. With the SYSLOG window open, you can select the following commands in the `Syslog` menu:
  - `Refresh`: updates the current SYSLOG file and displays it in the Syslog window.
  - `Save Syslog...`: stores the current display to a file.
  - `Load Syslog...`: lets you open and view a saved SYSLOG file.



Time	Source	Level	Message
00/00/0000 00:00:03	ADMIN	Notice	Interface INTRANET added, with IP address 0.0.0.0 and netmask 255.25
00/00/0000 00:00:03	ADMIN	Notice	Interface DMZ added, with IP address 0.0.0.0 and netmask 255.255.255
00/00/0000 00:00:39	ADMIN	Notice	Configuration download started from 192.168.100.99 via HTTPS
00/00/0000 00:00:39	ADMIN	Notice	Download from 192.168.100.99 via HTTPS succeeded
00/00/0000 00:00:56	ADMIN	Notice	Configuration download started from 192.168.100.99 via HTTPS
00/00/0000 00:00:57	ADMIN	Notice	Download from 192.168.100.99 via HTTPS succeeded
00/00/0000 00:01:37	ADMIN	Notice	Configuration upload started from 192.168.100.99 via HTTPS
00/00/0000 00:01:38	ADMIN	Notice	Upload from 192.168.100.99 via HTTPS succeeded
00/00/0000 00:01:39	ADMIN	Notice	IP address for INTRANET changed from 0.0.0.0 to 192.168.100.77
00/00/0000 18:05:09	ADMIN-LOGIN	Notice	Login from 192.168.100.99 via Telnet-SSL
00/00/0000 18:05:10	ADMIN-LOGIN	Notice	User from 192.168.100.99 via Telnet-SSL logged out
00/00/0000 18:08:29	ADMIN-LOGIN	Notice	Login from 192.168.100.99 via Telnet-SSL
00/00/0000 18:08:29	ADMIN-LOGIN	Notice	User from 192.168.100.99 via Telnet-SSL logged out
00/00/0000 18:10:18	ADMIN-LOGIN	Notice	Login from 192.168.100.99 via Telnet-SSL
00/00/0000 18:10:18	ADMIN-LOGIN	Notice	User from 192.168.100.99 via Telnet-SSL logged out

- ▶ WEBconfig, at the following location:

`System information : Syslog`



Idx.	Time	Source	Level	
1	01/01/1900 01:00:02	LOCAL2	Notice	Interface INTRANET added, with IP address 0.0.
2	01/01/1900 01:00:02	LOCAL2	Notice	Interface DMZ added, with IP address 0.0.0.0 an
3	01/01/1900 01:00:10	AUTH	Notice	local IP address for INTRANET is 192.168.2.50,
4	07/03/2011 18:07:57	LOCAL3	Alarm	Dst: 192.168.2.50:514 {Central_Office}, Src: 192
5	07/04/2011 11:13:46	LOCAL3	Alarm	last message repeated 1157 times
6	07/04/2011 12:01:54	LOCAL3	Alarm	Dst: 192.168.2.50:8612 {Central_Office}, Src: 19
7	07/04/2011 16:27:35	LOCAL3	Alarm	Dst: 192.168.2.50:8612 {Central_Office}, Src: 19
8	07/04/2011 16:37:05	LOCAL3	Alarm	Dst: 192.168.2.50:514 {Central_Office}, Src: 192
9	07/05/2011 13:16:07	LOCAL3	Alarm	last message repeated 103 times

Note: SYSLOG messages are written to the internal memory of the OpenBAT device if the device is configured as a SYSLOG client with the loopback address 127.0.0.1. In the LANconfig configuration file, you set this via the following path: `Configuration: Log & Trace : General`, Table `SYSLOG servers`

15.5.2 Structure of SYSLOG Messages

SYSLOG messages consist of three parts:

- Priority
- Header
- Contents

Priority

The priority in a SYSLOG message contains information about the importance of the message and the facility (i.e. the service or component that triggered the message). The following table shows the correlation between priority level, meaning and SYSLOG priority.

Priority	Meaning	SYSLOG priority
Alarm	This category includes all the messages that the system administrator has to check.	PANIC, ALERT, CRIT
Error	This level indicates all the error messages that can also occur during normal operation without the administrator having to act (e.g. connection errors).	ERROR
Warning	This level comprises messages that do not prevent the device from operating correctly.	WARNING
Information	This level comprises all messages of a purely informative character (e.g. accounting data).	NOTICE, INFORM
Debug	All debug messages. Debug messages create large data quantities and may prevent the device from operating correctly. Therefore, they should be deactivated during normal operation and only be used for troubleshooting.	DEBUG

The following table provides an overview of the meaning of all the internal message sources that you can set up in the OpenBAT device. The final column in the table also shows the standard assignment between the internal sources of the OpenBAT device and the SYSLOG facilities. You can change this assignment if required.

Source	Meaning	Facility
System	System messages (boot procedures, timer system, etc.)	KERNEL
Logins	Messages about a user's logins and logouts during the PPP negotiation and any errors that occurred in the process	AUTH
System Time	Messages about changes to the system time	CRON

Source	Meaning	Facility
Console logins	Messages about console logins (Telnet, Outband, etc.), logouts and any errors that occurred	AUTHPRIV
Connections	Messages about connections setups and terminations and any errors that occurred (e.g. display trace)	LOCAL0
Accounting	Accounting data after a connection is set up (users, online time, transfer volume)	LOCAL1
Management	Messages about configuration changes, remotely executed commands, etc.	LOCAL2
Router	Regular statistics about the most frequently used services (broken down by port number) and messages about filtered packets, routing errors, etc.	LOCAL3

Header

The header contains the name or the IP address of the device which sent the SYSLOG message. The chronological sequence is used to evaluate the messages. Time information is only added to the messages at the SYSLOG client in order not to disturb their chronological consistency due to different device times.

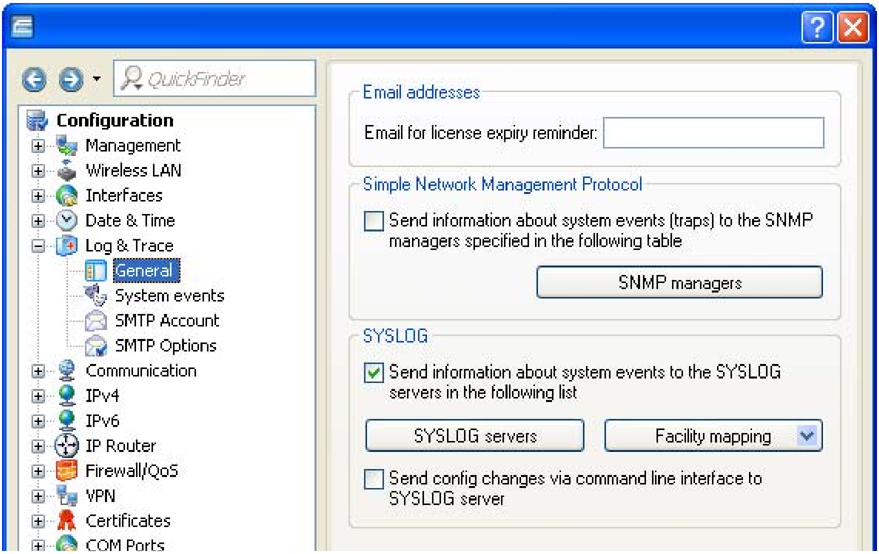
Note: The OpenBAT needs a valid time stamp for the evaluation of the SYSLOG messages in internal memory.

Contents

The actual contents of the SYSLOG messages describe the event, for example a login occurrence, the establishment of a WAN connection, or firewall activities.

15.5.3 Configuring SYSLOG with LANconfig

For configuration with LANconfig, the SYSLOG module is located under the configuration section `Log & Trace:General` on the "SYSLOG" pane.



Email addresses

Email for license expiry reminder:

Simple Network Management Protocol

□ Send information about system events (traps) to the SNMP managers specified in the following table

SYSLOG

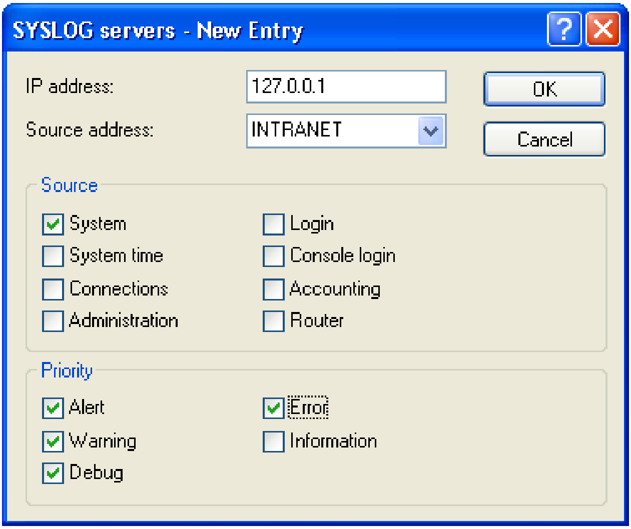
☑ Send information about system events to the SYSLOG servers in the following list

□ Send config changes via command line interface to SYSLOG server

Identifying SYSLOG Servers

Working from the SYSLOG dialog, above, you can open a configuration dialog for the identification of SYSLOG servers with which the device will communicate in its role as SYSLOG client, as follows:

- □ Click on the `SYSLOG servers...` button.
- □ In the ‘Syslog servers’ window, click `Add...` to open the ‘New Entry dialog:



SYSLOG servers - New Entry

IP address: 127.0.0.1

Source address: INTRANET

Source

☑ System
□ System time
□ Connections
□ Administration
□ Login
□ Console login
□ Accounting
□ Router

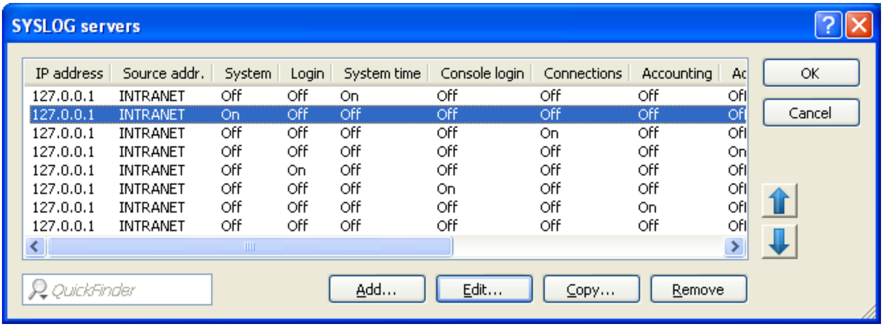
Priority

☑ Alert
☑ Warning
☑ Debug
☑ Error
□ Information

When setting up a SYSLOG client, you can configure the following parameters:

- IP Address:
  The IP address to which SYSLOG messages are to be sent.
- Source address:
  An optional, source address can be set here. This address is used instead of the IP address, above.
- Source:
  Select which of the internal OpenBAT sources are to send messages to this SYSLOG client.
- Priority
  You can further restrict the volume of messages by filtering on the basis of selected priorities.

The table of syslog servers (factory settings) is set up to display events that are relevant to diagnostics, and to save these to the internal syslog memory. The following screenshot shows these pre-defined SYSLOG servers in LANconfig:



IP address	Source addr.	System	Login	System time	Console login	Connections	Accounting	Ac
127.0.0.1	INTRANET	Off	Off	On	Off	Off	Off	Of
127.0.0.1	INTRANET	On	Off	Off	Off	Off	Off	Of
127.0.0.1	INTRANET	Off	Off	Off	Off	On	Off	Of
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	Off	On
127.0.0.1	INTRANET	Off	On	Off	Off	Off	Off	Of
127.0.0.1	INTRANET	Off	Off	Off	On	Off	Off	Of
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	On	Of
127.0.0.1	INTRANET	Off	Off	Off	Off	Off	Off	Of

Assignment of Internal Device Sources for SYSLOG Facilities

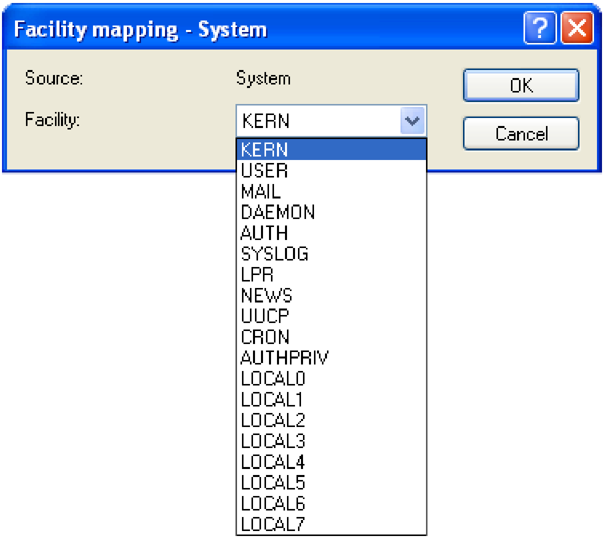
The SYSLOG protocol uses certain designations for message sources, the so-called facilities. Each internal source in the OpenBAT that can generate a SYSLOG message must therefore be assigned to a SYSLOG facility.

You can change the default assignment if required: In this way you can, for example, send all SYSLOG messages from a single device with the same facility (e.g. Local7) as specified. It is thus possible to collect all OpenBAT messages in a common log file by configuring the SYSLOG client appropriately.

To map a specific internal source to a facility, beginning in the SYSLOG dialog:

□ Click on the `Facility mapping` button, and select a device sourcefrom the drop-down list.

□ In the "Facility mapping" dialog, select a facility to associate with the source.



Source: System

Facility: KERN

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7

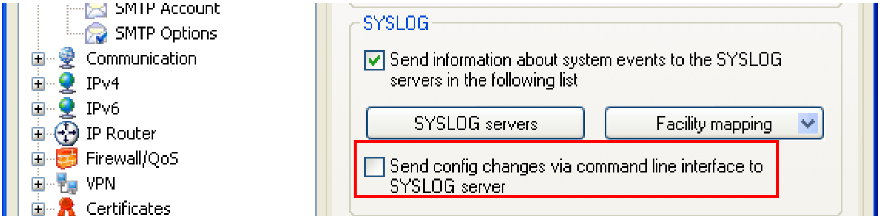
Logging Configuration Changes Made Via the Command Line

To meet the increased security requirements of network infrastructures, the devices are capable of logging to SYSLOG any changes to the configuration made via the command line interface. Configuration changes include any changes to the configuration parameters, executing actions, and uploading files such as certificates.

The devices write the following information to the SYSLOG:

- User name
- Name of the modified menu item or the executed action
- New value (or a notice that the change was not successful, e.g. due to a lack of permission)

In LANconfig, the settings for logging configuration changes made via the CLI console are to be found under `Log & Trace:General`.



☑ Send information about system events to the SYSLOG servers in the following list

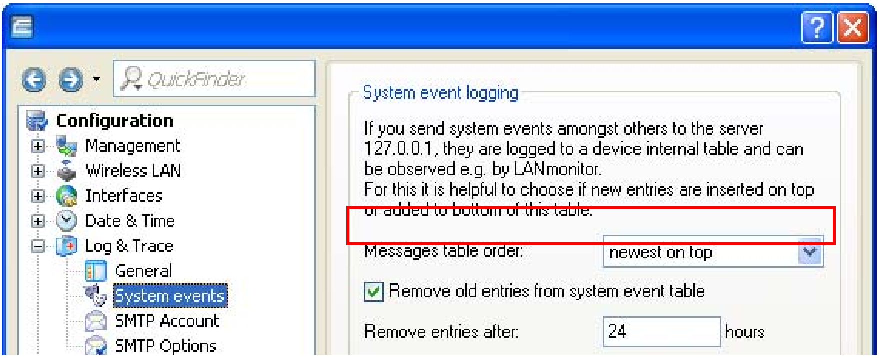
□ Send config changes via command line interface to SYSLOG server

Note: This protocol logs commands entered on the command line only. Configuration changes and actions made using LANconfig and WEBconfig are not logged.

Order of the system events

LANconfig allows you to control the order in which system events are displayed. By default the SYSLOG table displays the most recent messages at the top. You can optionally reverse the sorting order. The

You configure the sorting order in the dialog box `Log & Trace:System events` with the selection list "Message table order".



If you send system events amongst others to the server 127.0.0.1, they are logged to a device internal table and can be observed e.g. by LANmonitor.
For this it is helpful to choose if new entries are inserted on top or added to bottom of this table.

Messages table order: newest on top

☑ Remove old entries from system event table

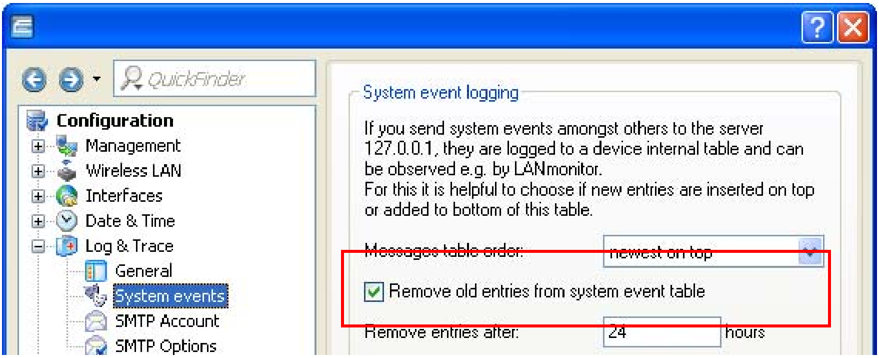
Remove entries after: 24 hours

Automatically delete SYSLOG entries

As of HiLCOS version 8.80, the devices are able to automatically delete old SYSLOG messages after a set retention period.

You configure this function in the dialog box `Log & Trace:System events`. The following settings are available:

- "Remove old entries from the system event table"
  Check this option to enable automatic deletion.
- "Delete entries after"
  In this field you set the time, in hours, after which the device is to delete the entries in the table.



System event logging

If you send system events amongst others to the server 127.0.0.1, they are logged to a device internal table and can be observed e.g. by LANmonitor.
For this it is helpful to choose if new entries are inserted on top or added to bottom of this table.

Messages table order: newest on top

☑ Remove old entries from system event table

Remove entries after: 24 hours

15.5.4 Configuring SYSLOG with Telnet or WEBconfig

You have the option of configuring the SYSLOG function for the OpenBAT device under the following path with Telnet or WEBconfig:

```
HiLCOS menu tree : Setup : SYSLOG
```

■ Parameters

The following parameters can be configured:

- Operating:
  Select ‘Yes’ to activate the dispatch of information about system events to the configured SYSLOG client.
- Port:
  The number of the port used for sending SYSLOG messages.
- Messages-Table-Order:
  Indicate how you want SYSLOG to be sorted in the table:
  oldest on top, or newest on top.

■ Facility Mapping

Select an item in the table to map each SYSLOG source to a facility.

■ Server table

Use the Server table to identify the servers with which the device will communicate in its role as SYSLOG client. Click the “Edit” button to modify the table, or click alternatively `Add` to create a new SYSLOG server item. Parameters include:

- IP Address:
  IP address of the SYSLOG client.
- Source:
  Source that caused the message to be sent. Enter the sum of the hexadecimal values for the selected sources:

Source name	Hex value	Source name	Hex value
System	1	Login	2
System time	4	Console login	8
Connections	10	Accounting	20
Administration	40	Router	80

- Level:
  SYSLOG level with which the message is sent. Enter the sum of the hexadecimal values for the selected levels:

Level name	Hex value
Alert	1
Error	2
Warning	4
Information	8
Debug	10

- Loopback address:
  An optional, source address can be set here. This address is used instead of the IP address, above.

All pre-defined SYSLOG clients transmit the messages to the IP address 127.0.0.1, i.e. to the OpenBAT itself. The sender IP address is the IP address from the "INTRANET" network. Individual entries have the following functions:

Index	Source	Level	Meaning
0001	4	0	System time without a specified level
0002	1	1f	System messages with the level alarm, error, alert or debug
0003	10	2	Connection messages with the level error
0004	40	8	Management messages with the level information
0005	2	a	Logins with the level error or information
0006	8	8	Console logins with the level information
0007	20	0	Accounting messages with the level information
0008	80	1	Router messages with the level alarm

For sources 4 and 20, the device doesn't send any SYSLOG messages to the internal SYSLOG memory in the default setting.

Delete Bootlog Manually

By entering the command `deletebootlog` anywhere on the command line you can manually delete the contents of the bootlog storage.

15.6 The Ping Command

With the ping command in Telnet or in a terminal connection an ‘ICMP Echo Request’ is sent to the addressed host. As long as the recipient provides the protocol and the request is not filtered by the firewall, the addressed host answers with an ‘ICMP Echo Reply’. If the host is not available, the last router before the host answers with a ‘Network unreachable’ or ‘Host unreachable’ response.

The syntax of the ping command is:

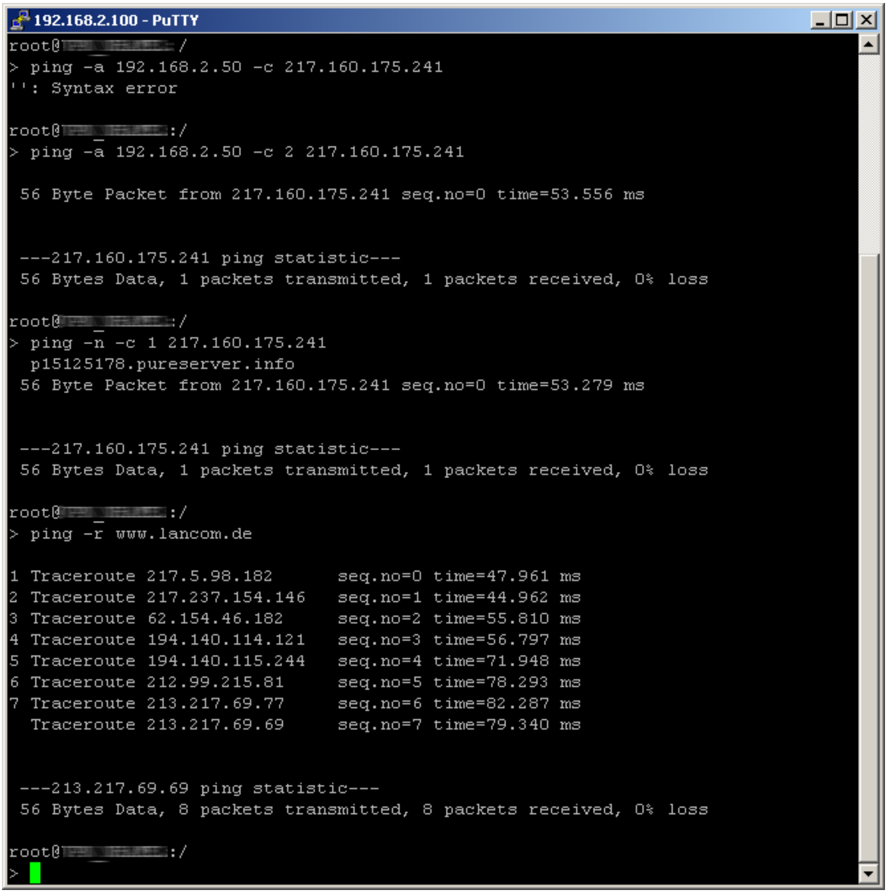
```
ping [-fnqr] [-s n] [-i n] [-c n] [-a a.b.c.d] hostaddress
```

The meaning of the optional parameters are listed in the following table:

Parameter	Meaning
-a a.b.c.d	Sets the sender address of the ping (standard: IP address of the router)
-a INT	Sets the intranet address of the router as sender address
-a DMZ	Sets the DMZ address of the router as sender address
-a LBx	Sets one of the 16 Loopback addresses as sender address. Valid for x are the hexadecimal values “0-f”
-6 <IPv6 Address> %<Scope>	Performs a ping command to the link-local address via the interface specified by <Scope>. For IPv6, the scope of parameters is of central importance: IPv6 requires a link-local address (fe80::/10) to be assigned to every network interface (logical or physical) on which the IPv6 protocol is enabled, so you must specify the scope when pinging a link-local address. This is the only way that the ping command knows which interface it should send the package to. A percent sign (%) separates the name of the interface from the IPv6 address. **Examples:** □ `ping -6 fe80::1%INTRANET` Ping the link-local address "fe80::1", which is accessible via the interface and/or the network "INTRANET". □ `ping -6 2001:db8::1` Pings the global IPv6 address '2001:db8::1".
-f	flood ping: Sends a large number of pings in a short time. Can be used to test network bandwidth, for example. Note: “flood ping” can easily be misinterpreted as a DoS attack.
-n	Returns the computer name of a specified IP address
-q	Ping command returns no output to the console (quiet)

Parameter	Meaning
-r	Changes to traceroute mode: The route taken by the data packets underway to the target computer is shown with all of the intermediate stations
-s n	Sets the packet size to n bytes (max. 1472)
-i n	Time between packets in seconds
-c n	Sends n ping signals
Host address	Address or host name of the target computer
stop /<RETURN>	Entering “stop” or pressing the RETURN button terminates the ping command

The following is an example of a series of ping commands:

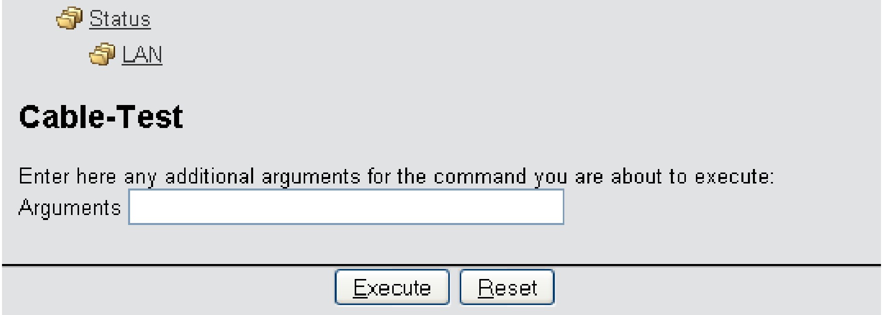


```
root@[redacted]/
> ping -a 192.168.2.50 -c 217.160.175.241
'': Syntax error

root@[redacted]:/
> ping -a 192.168.2.50 -c 2 217.160.175.241

 56 Byte Packet from 217.160.175.241 seq.no=0 time=53.556 ms


 ---217.160.175.241 ping statistic---
 56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@[redacted]:/
> ping -n -c 1 217.160.175.241
  p15125178.pureserver.info
 56 Byte Packet from 217.160.175.241 seq.no=0 time=53.279 ms


 ---217.160.175.241 ping statistic---
 56 Bytes Data, 1 packets transmitted, 1 packets received, 0% loss

root@[redacted]:/
> ping -r www.lancom.de

1 Traceroute 217.5.98.182      seq.no=0 time=47.961 ms
2 Traceroute 217.237.154.146   seq.no=1 time=44.962 ms
3 Traceroute 62.154.46.182     seq.no=2 time=55.810 ms
4 Traceroute 194.140.114.121   seq.no=3 time=56.797 ms
5 Traceroute 194.140.115.244   seq.no=4 time=71.948 ms
6 Traceroute 212.99.215.81     seq.no=5 time=78.293 ms
7 Traceroute 213.217.69.77     seq.no=6 time=82.287 ms
  Traceroute 213.217.69.69     seq.no=7 time=79.340 ms


 ---213.217.69.69 ping statistic---
 56 Bytes Data, 8 packets transmitted, 8 packets received, 0% loss

root@[redacted]:/
>
```

15.7 Cable Testing

You can use the WEBconfig software to test the cable connecting the device to a LAN or WAN. WEBconfig can detect a non-functioning cable even in the absence of any detected events. You can perform a cable test, in WEBconfig at the following location:

`HiLCOS menu tree : Status : LAN : Cable test`



Status

LAN

Cable-Test

Enter here any additional arguments for the command you are about to execute:

Arguments

To perform a cable test:

□ In the ‘Argument’ field, input the name of the device interface that you want to test, then click ‘Execute’.

□ To see the results of the test, navigate to the following location:

`HiLCOS menu tree : Status : LAN : Cable test results`

Possible test results include:

- OK:
  Cable plugged in correctly, line ok.
- open with distance ‘0m’:
  No cable plugged in, or interruption within less than 10 meters distance.

- open with indication of distance:
  Cable is plugged in, but the cable ceases to operate at the indicated distance.
- Impedance error:
  The pair of cables is not terminated with the correct impedance at the other end.

15.8 Data Packet Capture and Analysis

In order to capture packets for the analysis of errors or problems, HiLCOS version 8.60 and later features the command line tool "HiLCOScap". This command enables the capture of packets and writes the results to a file that you can open and analyze using a tool like Wireshark.

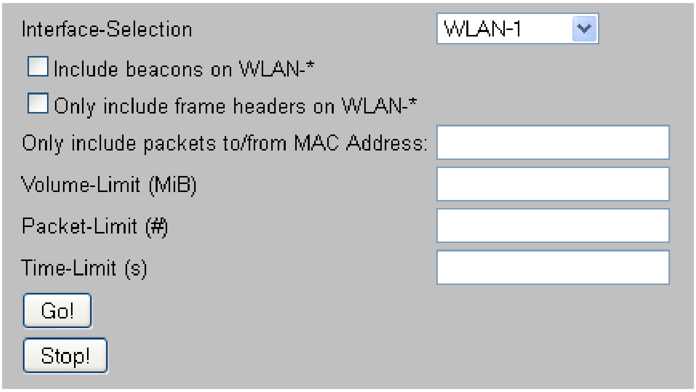
With HiLCOS version 8.80 an additional and more convenient method has been introduced: A new menu in WEBconfig allows you to set various parameters in order to capture data packets from selected interfaces and write these to a results file for subsequent analysis.

This method offers you several advantages:

- You do not need any special software, because you can run WEBconfig on any Web browser.
- There is no need to input any CLI commands. Instead, you work with a convenient menu.
- Operating WEBconfig over HTTPS ensures that the captured traffic remains confidential and secure.

15.8.1 Capture Data using Packet Capture

The `Extras:Packet capture` dialog offers you a simple way to record data packets from different interfaces and then use a software program (e.g. Wireshark) to analyze them.



Interface-Selection WLAN-1

□ Include beacons on WLAN-*

□ Only include frame headers on WLAN-*

Only include packets to/from MAC Address:

Volume-Limit (MiB)

Packet-Limit (#)

Time-Limit (s)

To specify the output file the following general menu items are available:

- "Interface selection":
  Use this drop-down menu to choose the interface that you want to record data packets for.
- "Include beacons on WLAN-*"
  Enable this option to capture the beacon information in addition to the data packets when the selected interface is a WLAN interface.
- "Only include frame headers on WLAN-*"
  Enable this option to restrict data-packet capture to the packet header when the selected interface is a WLAN interface.
- "Only include packets to/from MAC address":
  If you only want to record data packets for a particular physical address within the selected interface, you can specify it here.
- "Volume limit (MiB)":
  Enter the maximum volume of the recorded packages in Mebibytes.
- "Packet limit (#)":
  Here you can set the maximum number of packets to be recorded.
- "Time limit (s)":
  Enter the maximum time in seconds, after which the recording ends.

Click "Go!" to start the capture process. After a certain period of time—depending on the connection speed—a window opens for you to save the generated files. You can now save the file locally with the suffix *.cap. By default, the file name is composed of the description and interface associated with the device for which the data packets were recorded (e.g. MyDevice-LAN-2.cap). You can change the name when saving or later.

You can stop a recording at any time by clicking on "Stop!". This is useful if you initially need to enter, correct or adjust any parameters.

Note: If you start recording without setting any limits, the device keeps recording the packets until you manually stop the process by clicking on "Stop".

15.8.2 Capture Data using HiLCOSCAP

The “Wireshark” analysis tool analyzes the data traffic arising on a network connection and presents the results in graphical form. “Wireshark” analyzes either data for a current connection, or previously saved connection data. “HiLCOSCAP” allows you to record the data traffic and store it in a format compatible with Wireshark. You operate “HiLCOSCAP” via the command line by appending the corresponding parameter.
You control HiLCOSCAP using the following parameters:

- `-o`: Target file that contains the recording.
- `-p`: Password for the Hirschmann device on which HiLCOSCAP records the data traffic.
- `-i`: Interface of the Hirschmann device whose data HiLCOSCAP records.

  Note: If you leave out parameter `-i`, HiLCOSCAP outputs the interface list of the device.

- `-b`: Switch that also includes the beacons of the data traffic (only for WLAN).

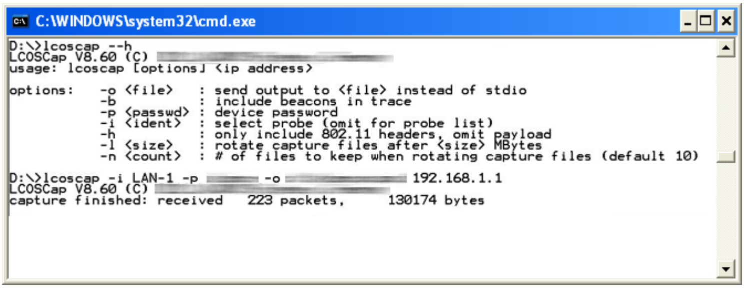
- `-h`: Switch that also includes the 802.11 header, but without a payload (only for WLAN).
- `-l`: Specifies the maximum size of the capture file. When the value specified is reached, HiLCOSCAP creates a new file. The files created are given sequential numbers.
- `-n`: Specifies the number of files that HiLCOSCAP creates. When the maximum number of files is reached, HiLCOSCAP overwrites the 1st file.

With `HiLCOScap --h` you call up the HiLCOSCAP help.
To record the data traffic of a device, enter the following command:

```
HiLCOScap -i LAN-1 -p Hirschmann -o d:/Hirschmann.pcap 192.168.1.1
```

- In this example, the device has the IP address “192.168.1.1”.
- The password is “Hirschmann”.
- You record the data traffic on interface “LAN-1”.
- The storage location and name of the file is `d:/Hirschmann.pcap`.

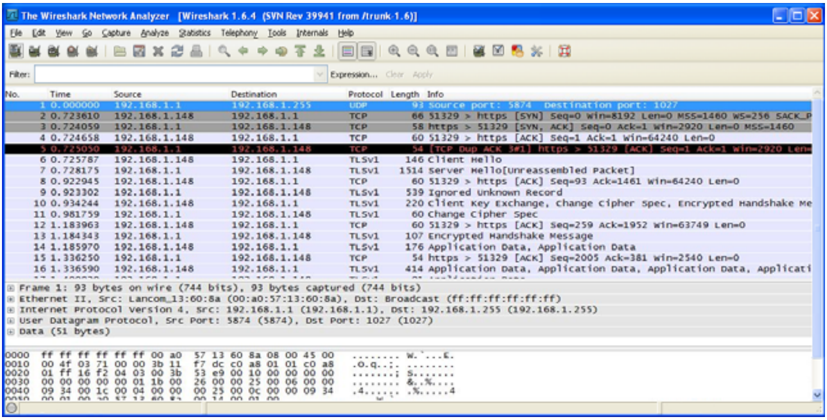
You use the key combination “Ctrl + C” to stop the recording.



```
D:\>lcoscap --h
LCOSCap V8.60 (C) [redacted]
usage: lcoscap [options] <ip address>

options:     -o <file>    : send output to <file> instead of stdio
             -b           : include beacons in trace
             -p <passwd>  : device password
             -i <ident>   : select probe (omit for probe list)
             -h           : only include 802.11 headers, omit payload
             -l <size>    : rotate capture files after <size> MBytes
             -n <count>   : # of files to keep when rotating capture files (default 10)

D:\>lcoscap -i LAN-1 -p [redacted] -o [redacted] 192.168.1.1
LCOSCap V8.60 (C) [redacted]
capture finished: received   223 packets,      130174 bytes
```

Figure 29: Recording the data traffic via the command line.

☐ You open the file created by HiLCOSCAP for analysis using “Wireshark”.



The Wireshark Network Analyzer [Wireshark 1.6.4 (SVN Rev 39941 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply

```
No.  Time      Source         Destination    Protocol Length Info
   1 0.000000  192.168.1.1    192.168.1.255  UDP        93 Source port: 5874  Destination port: 1027
   2 0.723610  192.168.1.148  192.168.1.1    TCP        66 51329 > https [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_P
   3 0.724059  192.168.1.1    192.168.1.148  TCP        58 https > 51329 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0 MSS=1460
   4 0.724658  192.168.1.148  192.168.1.1    TCP        60 51329 > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
   5 0.725050  192.168.1.1    192.168.1.148  TCP        54 [TCP Dup ACK 3#1] https > 51329 [ACK] Seq=1 Ack=1 Win=2920 Len=
   6 0.725787  192.168.1.148  192.168.1.1    TLSv1     146 Client Hello
   7 0.728175  192.168.1.1    192.168.1.148  TLSv1    1514 Server Hello[Unreassembled Packet]
   8 0.922945  192.168.1.148  192.168.1.1    TCP        60 51329 > https [ACK] Seq=93 Ack=1461 Win=64240 Len=0
   9 0.923302  192.168.1.1    192.168.1.148  TLSv1     539 Ignored Unknown Record
  10 0.934244  192.168.1.148  192.168.1.1    TLSv1     220 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Me
  11 0.981759  192.168.1.1    192.168.1.148  TLSv1      60 Change Cipher Spec
  12 1.183963  192.168.1.148  192.168.1.1    TCP        60 51329 > https [ACK] Seq=259 Ack=1952 Win=63749 Len=0
  13 1.184343  192.168.1.1    192.168.1.148  TLSv1     107 Encrypted Handshake Message
  14 1.185970  192.168.1.148  192.168.1.1    TLSv1     176 Application Data, Application Data
  15 1.336250  192.168.1.1    192.168.1.148  TCP        54 https > 51329 [ACK] Seq=2005 Ack=381 Win=2540 Len=0
  16 1.336590  192.168.1.148  192.168.1.1    TLSv1     414 Application Data, Application Data, Application Data, Applicati

⊞ Frame 1: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
⊞ Ethernet II, Src: Lancom_13:60:8a (00:a0:57:13:60:8a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 192.168.1.1 (192.168.1.1), Dst: 192.168.1.255 (192.168.1.255)
⊞ User Datagram Protocol, Src Port: 5874 (5874), Dst Port: 1027 (1027)
⊞ Data (51 bytes)

0000  ff ff ff ff ff ff 00 a0  57 13 60 8a 08 00 45 00   ........ W.`...E.
0010  00 4f 03 71 00 00 3b 11  f7 dc c0 a8 01 01 c0 a8   .O.q..;. ........
0020  01 ff 16 f2 04 03 00 3b  53 e9 00 10 00 00 00 00   .......; S.......
0030  00 00 00 00 00 01 1b 00  26 00 00 25 00 06 00 00   ........ &..%....
0040  09 34 00 1c 00 04 00 00  00 25 00 0c 00 00 09 34   .4...... .%.....4
```

Figure 30: File view with Wireshark

Enhancements in the menu system

- Packet capture
  You use this setting to manage the use of HiLCOSCAP to record the network data traffic.
  - **SNMP ID:**
    2.63
  - **Telnet path:**
    `Setup:Packet Capture`
- HiLCOSCAP operating
  With this setting you activate the HiLCOSCAP function.
  - **SNMP ID:**
    2.63.1
  - **Telnet path:**
    `Setup:Packet Capture:HiLCOSCap operating`
  - **Possible values:**
    Yes
    No
  - **Default:**
    Yes
- HiLCOSCAP port
  With this setting you specify the port used by HiLCOSCAP.
  - **SNMP ID:**
    2.63.2
  - **Telnet path:**
    `Setup:Packet Capture:HiLCOSCap port`
  - **Possible values:**
    5 characters from ‘0123456789’
  - **Default:**
    41047

A Index

B General Information

B.1 Maintenance

Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

B.2 Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very Good	**Good**	**Satisfactory**	**Mediocre**	**Poor**
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Comprehensive	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127/14-1600 or
- per mail to

Hirschmann Automation and Control GmbH
Department 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

C Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND